COPIA

COMUNE DI ANGUILLARA VENETA

Delibera della Giunta Comunale n. **91**

Oggetto: APROVAZIONE DEGLI INDIRIZZI E DELLE LINEE GUIDA E ATTI DI ADATTAMENTO DEL MODELLO ORGANIZZATIVO DEL COMUNE DI ANGUILLARA VENETA AL D.LGS N. 101/2018, RECEPIMENTO DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE E TRATTAMENTO DEI DATI PERSONALI.

L'anno duemiladiciannove addì trentuno del mese di ottobre alle ore 09:00 nella sala delle adunanze **SI E' RIUNITA LA GIUNTA COMUNALE** :

(P:presente A:assente)

BUOSO ALESSANDRA	SINDACO	P
BACCAGLINI GIAMPAOLO	VICESINDACO	P
SCARIETTO STEVE	ASSESSORE	P
BEDON IVO	ASSESSORE	P
MAGAGNA RAFFAELLA	ASSESSORE	P

Assiste alla seduta il/la Sig./ra RANZA GIORGIO, Segretario Comunale.
Il/la Sig./ra BUOSO ALESSANDRA nella sua veste di SINDACO assume la presidenza e riconosciuta legale l'adunanza dichiara aperta la seduta.

Verbale letto, approvato e sottoscritto.

Il Presidente	L'Assessore	Il Segretario. Comunale
F.to BUOSO ALESSANDRA	F.to BACCAGLINI GIAMPAOLO	F.to RANZA GIORGIO

REFERTO DI PUBBLICAZIONE Reg. Pubbl. N. 971 Si certifica, su conforme dichiarazione del messo, che in data odierna, copia di questa delibera é affissa all'Albo Pretorio per la pubblicazione di 15 giorni consecutivi
dal 06-11-2019 al 21-11-2019

IL FUNZIONARIO INCARICATO
F.to RUDAN DELIA

CERTIFICATO DI ESECUTIVITA': Si certifica che la presente deliberazione, non soggetta al controllo preventivo di legittimità , é stata pubblicata nelle forme di legge all'Albo Pretorio del Comune, senza riportare nei primi 10 giorni di pubblicazione denunce di vizi di legittimità o competenza, per cui la stessa **E' DIVENUTA ESECUTIVA** ai sensi del comma 3 dell'art. 134 del D.Lgs. 18.08.2000, n. 267.

data 18-11-2019

F.to IL FUNZIONARIO INCARICATO
RUDAN DELIA

La presente copia è conforme all'originale
Li, 06-11-2019

IL FUNZIONARIO INCARICATO
RUDAN DELIA

LA GIUNTA COMUNALE

PRESO ATTO:

- Che il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 2016/679 (GDPR- General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;
- Che, con il D.Lgs. n. 101/2018, in vigore dal 19 settembre 2018, il Codice della Privacy D.Lgs. n.196/2003 è stato adeguato al suddetto Regolamento UE;

- **RILEVATO:**
  Che le norme introdotte dal D.Lgs. n. 101/2018, di recepimento del Regolamento UE 2016/679, si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;
- Che appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;

RITENUTO pertanto opportuno:

- procedere alla definizione di un atto di indirizzo e linee guida che consentano all'Amministrazione di provvedere con immediatezza all'adattamento dell'organizzazione alle disposizioni contenute nel D.Lgs. n. 101/2018 di recepimento del Regolamento UE 2016/679 chiarendo e disciplinando gli aspetti rimessi alla propria autonomia organizzativa e procedimentale;
- prevedere un sistema di adattamento flessibile, graduale e continuativo alle disposizioni in materia anche tenuto conto dei successivi interventi sia normativi che dell'autorità di controllo nazionale;

RICHIAMATO IN PARTICOLARE:

- Lo Statuto comunale;
- Il vigente regolamento sull'ordinamento degli uffici e dei servizi;
- Il Dlgs n. 196/2003, come modificato dal D.Lgs. n. 101/2018;
- Il Dlgs n. 82/2005 e successive modificazioni ed integrazioni;
- L'art. 48 del D.Lgs. 18 agosto 2000 n.267 sulle competenze di questo organo in ordine all'approvazione del presente provvedimento;

VISTO il parere di regolarità tecnica del Responsabile dell'Area Amministrativa, ai sensi dell'art. 49 del D.Lgs. n. 267/2000;

DATO atto che si prescinde dal parere di regolarità contabile in quanto il presente atto non ha effetti finanziari diretti o indiretti;

RICHIAMATO altresì il vigente Regolamento di contabilità, approvato con Deliberazione consiliare n. 7 del 23.03.2016;

CON VOTI favorevoli unanimi resi in forma palese;

DELIBERA

1. **DI APPROVARE** gli indirizzi e le linee guida di adattamento del modello organizzativo del Comune di Anguillara Veneta al D.Lgs. n. 101/2018 di recepimento del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali di cui **all'allegato Sub A**, parte integrante del presente provvedimento;

2. **DI APPROVARE** il registro delle attività di trattamento (art. 30 del GDPR) di cui **all'allegato SUB B**, comprensivo del Piano di Conservazione dei Dati;

3. **DI APPROVARE** il Regolamento per l'utilizzo dei sistemi e strumenti informatici, di cui all'**allegato SUB C)**, parte integrante del presente provvedimento;

4. **DI APPROVARE** la Procedura di Data Breach, (art. 33 e 34 del GDPR) **allegato SUB D) e D1)**

5. **DI DARE ATTO** che la pubblicazione della presente Delibera all'albo on line del Comune, avviene nel rispetto della tutela alla riservatezza dei cittadini, secondo quanto disposto dalla normativa vigente in materia di protezione dei dati personali. Ai fini della pubblicità legale, l'atto destinato alla pubblicazione è redatto in modo da evitare la diffusione di dati personali identificativi non necessari, ovvero in riferimento ai dati sensibili;

6. **DI ASSOLVERE** l'obbligo di pubblicazione della presente Delibera, in conformità alle vigenti disposizioni in materia di pubblicità, trasparenza e diffusione di informazioni da parte delle Pubbliche Amministrazioni (D.Lgs. n. 33/2013 e s.m.i.), sul sito internet del Comune "Amministrazione Trasparente" – sezione "Provvedimenti" – sottosezione "Provvedimenti organi indirizzo politico", contestualmente alla pubblicazione dello stesso all'Albo Pretorio on line.

Oggetto: APROVAZIONE DEGLI INDIRIZZI E DELLE LINEE GUIDA E ATTI DI ADATTAMENTO DEL MODELLO ORGANIZZATIVO DEL COMUNE DI ANGUILLARA VENETA AL D.LGS N. 101/2018, RECEPIMENTO DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE E TRATTAMENTO DEI DATI PERSONALI.

PARERE DI REGOLARITA' TECNICA

Il sottoscritto **RUDAN DELIA,** responsabile del servizio interessato, ai sensi dell'art. 49, comma primo del T.U.E.L. n. 267/2000, per quanto concerne la **regolarità tecnica** esprime parere **Favorevole.**

IL RESPONSABILE DEL SERVIZIO

li, 31-10-2019

F.to **RUDAN DELIA**

Recommendations for a methodology of the assessment of severity of personal data breaches

Working Document, v1.0, December 2013

European Union Agency for Network and Information Security

www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This paper has been produced by experts of the Data Protection Authorities of Greece and Germany in collaboration with ENISA.

Editors

Clara Galan Manso (Seconded National Expert)

Sławomir Górniak

Contact

For contacting the authors please use sta@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like to thank the representatives of the Data Protection Authorities participating in the Article 29 Working Party Technology Subgroup for their valuable feedback which will help us further improve the methodology. We would also like to thank them for the submission of test cases which helped us evaluate the effectiveness of the methodology.

ISBN: 978-92-9204-078-9 DOI: 10.2824/27590

Acronyms

Art.29 WP – Working Party on the protection of individuals with regard to the processing of personal data

CB – Circumstances of the breach

DC – Data Controller

DPA – Data Protection Authority

DPO – Data Protection Officer

DPC – Data processing context

EI – Ease of identification

ENISA – European Union Agency for Network and Information Security

TS – Technology Subgroup (of the Art.29 WP)

Executive summary

The European Union Agency for Network and Information Security (ENISA) reviewed the existing measures and the procedures in EU Member States with regard to personal data breaches and published in 2011 a study on the technical implementation of the Art. 4 of the ePrivacy Directive, which included recommendations on how to plan and prepare for data breaches, how to detect and assess them, how to notify individuals and competent authorities and how to respond to data breaches. A proposal of a methodology for personal data breach severity assessment was also included as an annex to the above-mentioned recommendations, which was, however, not considered mature enough to be used at national level by the different Data Protection Authorities.

Against this background, the Data Protection Authorities of Greece and Germany in collaboration with ENISA developed, based on the above mentioned work, an updated methodology for data breach severity assessment that could be used both by DPAs as well as data controllers. This working document is a first result of the co-operation between experts of the two DPAs and ENISA. It is planned to further develop the methodology with the aim to generate a final practical tool for a data breach severity assessment.

An overview of the proposed methodology is presented in section 2 of this paper, and further elaborated in subsequent sections. Severity of a breach is defined as the estimation of the magnitude of potential impact on the individuals derived from the data breach. The core elements that have to be taken into account when assessing this severity are:

- Data processing context – type of breached data adjusted to the context in which they are used
- Ease of identification of the individual based on the data breached
- Circumstances of the breach, having additional influence on the severity of a breach

The methodology presented in this study is based on an as objective approach as possible whilst still being flexible enough to be adopted by various Data Protection Authorities by adjusting it to their size, national legal system and other factors. According to different requirements, the scoring of some categories can be adjusted to produce the most appropriate results.

Table of Contents

1 Introduction

1.1 Background information

With the amendment of Directive 2002/58/EC[1] (ePrivacy Directive) an obligation for the notification of personal data breaches by the providers of publicly available electronic communication services to competent authorities and affected individuals was introduced (art 4). The European Commission, as also stipulated in the Directive, has published implementing measures mainly on the format and circumstances of the personal data breach notification – Commission Regulation (EU) No 611/2013[2].

Following the provision of the ePrivacy Directive, a proposal for a general obligation of the data controllers for the notification of personal data breaches under certain conditions has been introduced in the draft Regulation on the Protection of Personal Data (art. 31) in the context of the overall Data Protection Reform Package[3].

Both these legislative provisions constitute important developments with the potential to increase the level of data security in Europe and foster reassurance amongst citizens on how their personal data are being secured and protected by data controllers. As part of the effective implementation of the data breach notification obligation, the Article 29 Working Party concluded, through its ePrivacy and technology subgroups, that there is a serious need for the development of a methodology for the assessment of the severity of personal data breaches. The discussions within the Article 29 Working Party are currently still ongoing.

The European Union Agency for Network and Information Security (ENISA) reviewed the already existing measures and the procedures in EU Member States with regard to personal data breaches and published in 2011 a report on the technical implementation of the Art. 4 of the ePrivacy Directive[4]. A proposal of a methodology for personal data breach severity assessment was included as an annex to that report, which was, however, not considered as mature enough to be used at national level by the different Data Protection Authorities.

Against this background, the Data Protection Authorities of Greece and Germany in collaboration with ENISA developed, based on the above mentioned work, an updated methodology for data breach severity assessment that could be used both by DPAs as well as data controllers. This working document is a first result of the co-operation between experts of the two DPAs and ENISA. It is planed to further develop the methodology with the aim to generate a final practical tool for a data breach severity assessment.

1.2 Objectives

The proposed methodology presented in this document has been designed with the following objectives:

- To provide data controllers with a quantitative tool (to the extent that this is possible) to assess the severity of data breaches and accordingly notify the competent authorities as well as the

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:01:EN:HTML
[2] http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2013:173:SOM:EN:HTML
[3] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
[4] Recommendations on technical implementation guidelines of Article 4, http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

affected individuals. The tool could also serve as a means for data controllers to quickly determine the necessary mitigation measures.

- To provide the national competent authorities with a tool to assess the severity of the breaches notified by the data controllers.
- To support the national competent authorities in the process of performing detailed analyses and statistics concerning the reported personal data breaches.
- To contribute to the harmonization of the severity assessment of personal data breaches in the European Union, by proposing a common methodology and severity scoring. This would be especially important in the case of cross-border breaches.

1.3 Severity of data breaches

The severity of a personal data breach is defined, in the context of this methodology, as the ***"estimation of the magnitude of potential impact on the individuals derived from the data breach"***.

As stipulated in Directive 2009/136/EC[5] (recital (61)), the impact of a personal data breach may include "for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision of publicly available communications services in the Community".

With the use of this methodology the data controller is guided through the process by specific quantitative criteria in order to make the overall assessment. The same criteria can be used by the competent authorities, together with the information provided by the controller in the notification form[6], in order to make its own assessment of the breach.

It should be noted that the controller is applying the methodology using the information that is in his/her possession at the time of the breach. In that sense, the methodology cannot always cover all the possible casuistic, including likely impacts on specific groups of individuals or very special cases that cannot be fully addressed under a general methodology. Therefore, it has to be reminded that both, data controllers and competent authorities should put particular care when dealing with cases that, because of their specificities, could not be rightly assessed using this methodology.

[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

[6] An example of a template of a data breach notification form to the competent authorities is available in the Appendix A of http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

2 Overview of the methodology

2.1 Criteria

The main criteria taken into account while assessing the severity of a personal data breach are:

- **Data Processing Context (DPC):** Addresses the type of the breached data, together with a number of factors linked to the overall context of processing.
- **Ease of Identification (EI):** Determines how easily the identity of the individuals can be deduced from the data involved in the breach.
- **Circumstances of breach (CB):** Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent.

2.2 Calculation of the severity

Based on the above criteria, the approach of this methodology is the following:

- DPC is at the core of the methodology and evaluates the criticality of a given data set in a specific processing context.
- EI is a correcting factor of the DPC. The overall criticality of a data processing can be reduced depending on the value of EI. In other words, the lower the ease of identification is, the lower gets the overall score. Therefore, the combination of the EI and DPC (multiplication) gives the initial score of the severity (SE) of the data breach.
- CB quantifies specific circumstances of the breach that may be present or not in a particular situation. So, when present, CB can only add to the severity of a specific breach. For this reason the initial score can be further adjusted by the CB.

Thus, the final score of the severity assessment can be extracted using the following formula:

$$SE = DPC \times EI + CB$$

In this way, in order for the controller to get the severity result, all three criteria should be scored.

The result belongs to a certain range of values which corresponds to one of the four severity levels: low, medium, high and very high[7]. At the end of the assessment, other possibly relevant criteria (number of individuals and unintelligibility of data) that have not been considered in the methodology are evaluated and flagged to the competent authority when applicable.

It is essential to bear in mind that all scores and/or rankings used in this methodology were solely set for the use within the severity formula. They are not meant to bear any significance to a conclusion about the weighting or ranking of certain types of data in general, let alone an indication to any legal consequences or precedents as to the use of this data for other purposes.

[7] Severity levels will be explained in details in section 3.2.

3 Detailed description of scoring and severity levels

3.1 Scoring of the criteria

3.1.1 Data Processing Context (DPC)

In order to define the score for DPC, the data controller should follow the next steps:

- Step 1: Definition and classification of the types of personal data

  a) Define the types of the personal data involved in the breach.

  b) Classify the data in at least one of the four categories: simple, behavioural, financial, and sensitive data (these categories are explained in details in Annex 1). In this way a preliminary basic DPC score is obtained.

  The list of data types described under the four categories is not exhaustive; however most data involved in real cases can be matched to at least one of the categories. Credentials are not considered as a specific data category and should be handled based on the type of data processed by the systems where they provide access to.

- Step 2: Adjustment by contextual factors related to the data processing

  c) Assess the occurrence of certain factors that could increase or decrease the basic score (data volume, special characteristics of the controllers or the individuals, invalidity/inaccuracy of data, public availability (before the breach), nature of data).

  d) In case such factors exist, accordingly increase/decrease the basic score. Assessment Table 1 provides the adjustment scales per category of data, together with example cases that could lead to lower/higher scores.

Please refer to the Annex 1 for a list of contextual factors and specific examples of DPC scoring.

Note: Even though, for the purpose of the methodology, four data categories are ranked, the categorization itself is not to be seen as a general ranking of the types of data at hand. Much more, additional contextual factors related to the data always need to be taken into account when regarding the processing of a certain type of data. Therefore, the basic score is to be seen just as a general indication of the criticality connected to a certain category of data and the DPC scoring of any data type can always vary from 1 to 4.

If the data matches more than one category the above mentioned steps have to be followed for each category applicable. In these cases the value to use for the overall calculation of the severity will be the highest score reached.

If the controller chooses to alter the DPC basic score (within the range of Assessment Table 1), the new score has to be supported by an explanation describing the particular contextual factors of the breach and their influence.

3.1.2 Ease of identification (EI)

Ease of identification (EI) evaluates how easy it will be for a party who has access to the set of data to univocally match them to a certain person.

For the purpose of this methodology we have defined four levels of EI (negligible, limited, significant and maximum) with a linear increase in score. The lowest score is given when the possibility to identify the individual is negligible, meaning that it is extremely difficult to match the data to a particular person, but still it could be possible under certain conditions. The highest score is selected when identification is possible directly from the data breached with no special research needed to discover the individual's identity. Annex 2 describes these levels in details.

When defining EI, it should be taken into account that identification may be directly (e.g. on the basis of a given name) or indirectly (eg. on the basis of ID number) possible from the breached data, but may also depend on the specific context of the breach. Therefore, certain identifiers may lead to different EI scores according to the specific case of the breach.

Please refer to the Annex 2 for specific examples of EI scoring using common identifiers.

In addition, when defining EI the controller should take into account all the means likely reasonably to be used by any person to identify the individuals. This includes information that is public, held or obtained otherwise, including over the Internet, as well as possible cross-matching with other sources than can be accessed by the data controller or a third party.

3.1.3 Circumstances of the breach (CB)

The elements that are considered under CB are the loss of security (confidentiality, integrity, availability) and malicious intent and are complementary to DPC and EI, as follows:

Loss of confidentiality: Loss of confidentiality occurs when the information is accessed by parties who are not authorized or don't have a legitimate purpose to access it. The extent of loss of confidentiality varies by the scope of disclosure, i.e. the potential number and type of parties that may have unlawfully access to the information.

Loss of integrity: Loss of integrity occurs when the original information is altered and substitution of data can be prejudicial for the individual. The most severe situation occurs when there are serious possibilities that the altered data have been used in a way that could harm the individual.

Loss of availability: Loss of availability occurs when the original data cannot be accessed when there is a need for it. It can be either temporal (data are recoverable but it will take a period of time and this can be detrimental for the individual), or permanent (data cannot be recovered).

Malicious intent: This element examines whether the breach was due to an error or mistake, either human or technical, or it was caused by an intentional action of malicious intent. Non malicious breaches include cases of accidental loss, inadequate disposal, human error and software bug or misconfiguration. Malicious breaches include cases of theft and hacking aiming to harm the individuals (e.g. by exposing their personal data to unauthorised third parties). In other cases malicious intent might include transfer of personal data to third parties for profit (e.g. selling of lists of personal data). In some cases malicious intent could also be inferred from actions aiming to harm the data controller (e.g. through stealing and exposing the personal data to unauthorized parties). Malicious intent is a factor that increases the likelihood that the data is used in harmful way, since this was the initial purpose of the breach.

With regard to CB scoring, contrary to DPC and EI where the maximum score reached is chosen, the points obtained for each CB element are added to obtain the final score, as different circumstances can occur in the same breach. Assessment Table 3 provides different scores per CB element and for different types of circumstances.

Please refer to the Annex 3 for specific examples of CB scoring.

3.2 Definition of severity level

As introduced in the Section 2.2, the overall severity (SE) is calculated by the following formula:

$$SE = DPC \times EI + CB$$

The final score shows the level of severity of a certain breach, taking into account the impact to the individuals[8].

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

3.3 Flags

Once the severity level has been defined, it can be accompanied by flags indicating certain elements of the breach that, although they do not affect a priori the scoring, they are important for the final assessment. For the purpose of the methodology, two flags have been considered:

Number of individuals breached exceeds 100. Data of an individual, breached in the context of a bigger incident, can potentially be more easily disclosed, whereas at the same time a high number of affected individuals influences the overall scale of the breach.

Data unintelligible. Unintelligibility (e.g. in the form of strong encryption and without key compromise) can substantially decrease the impact to individuals, since it highly decreases the possibility of unauthorized parties accessing the data.

[8] Table setting the levels of severity of a data breach was first introduced in the "Recommendations on technical implementation guidelines of Article 4", page 24, but has been made more precise in this document.

4 Use of the methodology

4.1.1 Notification to competent authorities

The severity level of the breach (together with the flags), as calculated through this methodology, could be integrated in the notification sent by the controller to the competent authorities. This can be done either automatically in the notification template or through the use of a standalone tool. The competent authorities will be free to evaluate the result (using the same template/tool and the information provided by the controller) and accept it or reject it, following their own assessment.

If for some reason the final severity level is deemed to be incorrect by the data controller, it could be possible for the controller to state the "correct" level, including his/her arguments for the different result, in a free text box (ex. integrated in the notification form). Moreover, any change in the default score for the DPC criterion should also be explained by the controller using a free text box. These boxes could also be used to leave comments without changing the severity level.

4.1.2 Notification to the individuals

The severity level could be used by the controller and the competent authority to determine if there is a need to notify the individuals. The level upon which notification should be deemed necessary could be mutually accepted by all competent authorities or vary depending national-wide criteria.

5 Closing remarks

On the previous pages we have presented a working document on our proposed methodology for assessing data breaches. This proposal ultimately aims towards being integrated into a notification template (such as in ENISA's Recommendations for the technical implementation of the Art.4 of the ePrivacy Directive[9]) to achieve an as far as possible automated severity assessment.

The methodology presented in this study is based on an as objective approach as possible whilst still being flexible enough to be adopted by various Data Protection Authorities by adjusting it to their size, national legal system and other factors. According to different requirements, the scoring of some categories can be adjusted to produce the most appropriate results:

- Data processing context can be adjusted according to the importance of data (simple, behavioural, financial etc.) assigned by the specific DPA
- Ease of identification can take into account the reality in a given country and its legal system (public availability of personal numbers, names, addresses etc.)
- Circumstances of a breach offer the highest flexibility to adjust the final result to the needs of a DPA
- Flags can either be adjusted (for example in function of records breached), complemented by new ones or moved to the CB (circumstances of a breach) table.

ENISA and the DPAs of Greece and Germany aim at further developing the work presented in this document with the final scope of publishing a practical data breach severity tool that can be useful both for the DPAs and the data controllers across the EU.

[9] http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn/art4_tech

Annex 1 – Data processing context

A1 Assessment tables

Table 1: Data Processing Context (DPC)		Score
Simple data	Eg. biographical data, contact details, full name, data on education, family life, professional experience, etc.	
	Preliminary basic score: when the breach involves ''simple data'' and the controller is not aware of any aggravating factors.	**1**
	The DPC score could be increased by 1, e.g. when the volume of "simple data" and/or the characteristics of the controller are such that certain profiling of the individual can be enabled or assumptions about the individual's social/financial status can be made.	2
	The DPC score could be by 2, e.g. when the "simple data" and/or the characteristics of the controller can lead to assumptions about the individual's health status, sexual preferences, political or religious beliefs.	3
	The DPC score could be increased by 3, e.g. when due to certain characteristics of the individual (e.g. vulnerable groups, minors), the information can be critical for their personal safety or physical/psychological conditions.	4
Behavioural data	Eg. location, traffic data, data on personal preferences and habits, etc.	
	Preliminary basic score: when the breach involves ''behavioural data'' and the controller is not aware of any aggravating or lessening factors.	**2**
	The DPC score could be decreased by 1, e.g. when the nature of the data set does not provide any substantial insight to the individual's behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).	1
	The DPC score can be increased by 1, e.g. when the volume of "behavioural data" and/or the characteristics of the controller are such that a profile of the individual can be created, exposing detailed information about his/her everyday life and habits.	3
	The DPC score can be increased by 2, e.g. if a profile based on individual's sensitive data can be created.	4

Financial data	Any type of financial data (e.g. income, financial transactions, bank statements, investments, credit cards, invoices, etc.). Includes social welfare data related to financial information.	
	Preliminary basic score: when the breach involves ''financial data'' and the controller is not aware of any aggravating or lessening factors.	**3**
	The DPC score could be decreased by 2, e.g. when the nature of the data set does not provide any substantial insight to the individual's financial information (e.g. the fact that a person is the customer of a certain bank without further details).	1
	The DPC score could be decreased by 1, e.g. when the specific data set includes some financial information but still does not provide any significant insight to the individual's financial status/situation (e.g. simple bank account numbers without further details).	2
	The DPC score could be increased by 1, e.g. when due to the nature and/or volume of the specific data set, full financial (e.g. credit card) information is disclosed that could enable fraud or an detailed social/financial profile is created.	4
Sensitive data	Any type of sensitive data (e.g. health, political affiliation, sexual life)	
	Preliminary basic score: when the breach involves 'sensitive data'' and the controller is not aware of any lessening factors.	**4**
	The DPC score could be decreased by 1, e.g. when the nature of the data set does not provide any substantial insight to the individual's behavioural information or the data can be collected easily (independently from the breach) through publicly available sources (e.g. combination of information from web searches).	1
	The DPC score could be decreased by 2, e.g. when nature of data can lead to general assumptions.	2
	The DPC score could be decreased by 1, e.g. when nature of data can lead to assumptions about sensitive information.	3

A2 Description of contextual factors to be considered in DPC scoring

Increasing factors:

- ✓ **The volume of the breached data (for the same individual)**: this factor can increase the basic DPC score, due to the increment of the quantity of the breached information (i.e. acting as aggravating factor). The volume should be considered both in terms of time (e.g. same type of data over a certain period of time) and content (complementing data of the same type). For example, in case of a breach of traffic data at an ISP, the DPC score would be higher (for the same individual) if the data cover a period of one year than if they are limited to one week (time). As another example, in case of a breach at a bank, the DPC score of the complete file of an individual would be higher than that of a single document from the same file (content).
- ✓ **Special characteristics of the data controller**: this factor relates to the field of operation and the activities of the data controller, which could increase the basic DPC score of the data, revealing additional information for a certain data set. For example, the DPC score of a customers' list would be higher if it comes from an online pharmacy than from a stationery shop.
- ✓ **Special characteristics of the individuals**: the basic DPC score of a certain data set could also be increased in case that the individuals belong to a social group with particular needs (e.g. minors, individuals of a particular group with special characteristics). For example, the DPC score of a list of telephone numbers would increase if it concerns known members of the national parliament.

Decreasing factors:

- ✓ **Invalidity/inaccuracy of the data**: the basic DPC score of a certain data set can be decreased if the invalidity or inaccuracy of the data is known to the controller (e.g. due to their age or content) and, thus, their significance is reduced. The controller needs to be certain of this circumstance to include it in the assessment. For example a postal service's list of addresses where letters could not be delivered would be considered as inaccurate (i.e. most probably the individuals have moved to another address).
- ✓ **Public availability**: the basic DPC score of a data set can also be decreased in case the breached data were already publicly available before the breach or can be easily collected and/or accessed through publicly available sources.
- ✓ **Nature of data**: another decreasing factor could in some cases be the very nature of a particular data set that, despite its initial DPC scoring, is of lower significance, in terms of the information that it can reveal about the individual. This is, for example, the case of a medical certificate that is just certifying that the individual is in a good state of health without disclosing any other information. In this case, although the basic score would be 4 due to health data being sensitive data, the specific data set's final DPC score would be 1, as it cannot per se affect the individual's personal life. This factor, however, should be considered with great care and clear explanation of the reason why a particular data processing is by nature lower than its basic DPC score.

A3 Examples of DPC scoring/adjustment per category of data

Simple data

Example 1: List of names and telephone numbers

- **Case 1: the list is the customer list of a supermarket/restaurant.**

  Score = 1 (no alteration due to contextual factors)

- Case 2: the list comes from a company selling luxury cars/homes.

  Score = 2 (by characteristics of controller leading to assumptions about financial/social status)

- Case 3: the list comes from a specialized electronic pharmacy selling products for patients with diabetes.

  Score = 3 (by characteristics of controller leading to assumptions about the individual's health status)

- Case 4: the list includes the names of people working undercover for secret police.

  Score = 4 (by characteristics of individuals that could be critical for their personal safety)

Example 2: A professional CV database

- **Case 1: the data come from an online career site where access to CVs is available for registered users.**

  Score = 1 (no alteration due to contextual factors)

- Case 2: the data come from an organization helping unemployed people to find employment.

  Score = 2 (by characteristics of controller leading to assumptions about financial/social status)

- Case 3: the data come from an institution supporting gay people rights.

  Score = 3 (by characteristics of controller leading to assumptions about the individual's sexual life).

- Case 4: the data come from an organization helping recovering drug addicts to find employment.

  Score = 4 (by characteristics of individuals that could cause them serious damage).

Example 3: List of names and postal addresses

- **Case 1: the list is the customer list of a flower shop.**

  Score = 1 (no alteration due to contextual factors)

- Case 2: the list comes from an investment bank.

  Score = 2 (by characteristics of controller leading to assumptions about financial/social status)

- Case 3: the list is the delivery addresses of an adult books store.

  Score = 3 (by characteristics of controller leading to assumptions about the individual's sexual preferences)

- Case 4: the list concerns persons that have been accused for child abuse.

  Score = 4 (by characteristics of individuals that could cause them serious damage)

Behavioral data

Example 1: Telephone call history (traffic data – no content)

- Case 1: the data come from the helpdesk of an ISP and include incoming calls from subscribers to the helpdesk regarding technical problems.

  Score = 1 (by nature of the data set).

- **Case 2: the data come from an ISP and include subscribers' call history of the last week.**

  Score = 2 (no alteration due to contextual factors)

- Case 3: the data come from an ISP and include subscribers' call history of the last year.

  Score = 3 (a detailed profile of the individual can be created).

- Case 4: the data come from a psychological support centre for people suffering from a serious illness and includes incoming calls.

  Score = 4 (by characteristics of controller disclosing health status).

Example 2: Data in a fidelity card

- Case 1: the card is from a supermarket and includes only the number of points gained from purchases.

  Score = 1 (by nature of the data set).

- **Case 2: the card is from a supermarket and includes information on purchase history for the last month.**

  Score = 2 (no alteration due to contextual factors).

- Case 3: the data come from a transportation card and includes information about location/movements over the last year.

  Score = 3 (a detailed profile of the individual can be created).

- Case 4: the card is from a pharmacy and includes information on recent purchases of medical products.

  Score = 4 (by nature of data set disclosing sensitive data).

Example 3: Data from a social network

- Case 1: the data are publically available on the internet (e.g. pictures that the user has published online).

  Score = 1 (by public availability).

- **Case 2: the data include information about the user's preferences and everyday life of the last month that the user has shared with his/her friends (e.g. information published on user's wall).**

  Score = 2 (no alteration due to contextual factors).

- Case 3: the data include information about the user's preferences and everyday life of the last year that the user has shared with his/her friends (e.g. information published on user's wall).

Score = 3 (a detailed profile of the individual can be created).

- Case 4: the data include personal communication (e.g. personal messages) that may expose information about users' sexual life or health status.

  Score= 4 (leads to detailed profiling related to sensitive data).

Financial data

Example 1: Bank statements

- Case 1: the data come from a bank and include only a letter, through which the individual is identified as a client without providing any information about the specific relations between the client and the bank (e.g. only his/her name and address but no account number or information about transactions).

  Score = 1 (by nature of the data set).

- Case 2: the data come from a bank and include only a transactions history of one day without further details (e.g. account number, name and transaction).

  Score = 2 (by nature of data, info that can lead to limited information about financial behaviour).

- **Case 3: the data come from a bank and concern account balances of clients of the last month.**

  Score = 3 (no alteration due to contextual factors).

- Case 4: the data come from a bank and include account balances of clients of the last year, showing all transactions and related with them details.

  Score = 4 (by volume and nature of data leading to profiling)

Example 2: Income declaration

- Case 1: the data contains a statement to confirm that the individual has submitted his/her income declaration.

  Score = 1 (by nature of the data set).

- Case 2: the data contains the percentage of the taxation which the individual must pay.

  Score = 2 (by nature of data, info that can lead to limited information about financial status).

- **Case 3: the data contains all the fields of one year income declaration of the individual.**

  Score = 3 (no alteration due to contextual factors).

- Case 4: the data contains all the fields of the income declaration of the individual for the last 10 years.

  Score = 4 (by volume and nature of data leading to detailed profiling).

Example 3: Credit card information

- Case 1: the data come from a bank and contain credit card details of individuals but these data are more than ten years old and therefore these cards are not valid.

  Score = 1 (by age of the data set).

- Case 2: the data come from an online shop and contain some credit card information of individuals, but not the necessary set of details to perform financial transactions.

  Score = 2 (by nature of data, info that can lead to limited information about financial status).

- **Case 3: the data come from a bank and contain some credit card information of individuals, but not the necessary set of details to perform financial transactions. However, they contain information about certain purchases of the individuals for the period of one year.**

  Score = 3 (no alteration due to contextual factors).

- Case 4: the data come from an online shop and contain full credit card details that can be used for financial transactions.

  Score = 4 (the data set could be used for fraud).

Sensitive data

Example 1: Data on blood analysis

- Case 1: the data come from a laboratory and include only an indication that the data individuals have performed general blood tests.

  Score = 1 (by nature of data).

- Case 2: the data come from a laboratory of an emergency room of a hospital and only include information about the fact that the individuals performed blood tests (without further details).

  Score = 2 (by nature of data leading to general assumptions).

- Case 3: the data come from a laboratory and includes an indication that the individuals have performed test for a certain disease, without indication of results. Score = 3 (by nature of data leading to assumptions that could cause damage to the individual).

- **Case 4: the data come from a laboratory and includes results of the tests.**

  Score = 4 (no alteration due to contextual factors).

Example 2: Data on political affiliation

- Case 1: the data come from a major political party and include names of prominent members who hold public positions and their affiliation with the party is publically known.

  Score = 1 (by nature of data).

- Case 2: the data come from a company organizing events and include the names of individuals that attended a charity event sponsored by a specific political party.

  Score = 2 (by nature of data leading to general assumptions).

- Case 3: the data come from a political party and include the names of individuals that attended a specific conference organised by the party.

  Score = 3 (by nature of data leading to assumptions that could cause damage to the individual).

- **Case 4: the data come from a closed internet forum and include the political opinions expressed by the members of the forum.**

  Score = 4 (no alteration due to contextual factors).

Example 3: Data on sexual life

- Case 1: the data come from an online discussion forum about relationships and include only the name of registered users without any further information.

  Score = 1 (by nature of data).

- Case 2: the data come from a dating site and include only the name of customers without any further information.

  Score = 2 (by nature of data leading to general assumptions).

- Case 3: the data come from a dating site specialized, but not exclusive, in heterosexual or gay dating and include the name of customers.
- Score = 3 (by nature of data leading to assumptions about sensitive information).
- **Case 4: the data come from a dating site and include the declared sexual orientation of customers.**

  Score = 4 (no alteration due to contextual factors).

Credentials

Example: Username and password of registered users in an online service

- Case 1: the credentials are used for accessing users' accounts in an electronic music store.

  Score = 1 / Simple data (no alteration due to contextual factors)

- Case 2.1: the credentials are used for access to users' accounts in a supermarket's web site, including information about previous shopping lists.

  Score = 2 / Behavioural data (no alteration due to contextual factors)

- Case 2.2: the credentials are used for access to user's accounts in a social media site.

  Score = 3 / Behavioural data with detailed profiling

- Case 3.1: the credentials can be used for access to user's account in the national tax system, proving information about users' income.

  Score = 3 / Financial data (no alteration due to contextual factors)

- Case 3.2: the credentials can be used for online banking with the possibility to perform financial transactions (e.g. transfer of money).

  Score = 4 / Financial data with full financial information and possibility for fraud.

- Case 4: the credentials are used for access to users' accounts in an online community related to sexual preferences.

  Score = 4 / Sensitive data (no alteration due to contextual factors)

Annex 2 – Ease of identification (EI) scoring

This annex will present the examples of EI scoring for common identifiers.

Identification can be direct or indirect and is performed with the use of certain identifiers, taking also into account the overall context of the processing of personal data. The next examples show a (non-exhaustive) list of common identifiers and different cases of their possible use for EI scoring.

It should be noted that in many cases the breach will include a combination of different identifiers, which automatically increases the ease of identification. This is a very important element that should be taken into account by the controller and is reflected in the examples below.

Full name (first name, surname)

It is considered as the most common direct identifier but EI score may vary depending on the case, since the full name does not always in itself uniquely single out the individual. For example, when identification is performed using only the individual's full name:

- EI = 0,25 (Negligible) throughout a country's population where many people share that same full name
- EI = 0,5 (Limited) throughout a country's population where few people share that same full name.
- EI = 0,75 (Significant) throughout a small city's population where few or no people share that same full name.
- EI=1 (Maximum) throughout a country's population using also date of birth and email address.

ID card/passport/social security number

They are all considered as unique identifiers and they can be used to single out the individual, as long as it is possible to link them to a reference database (e.g. linking an ID card to a particular person). For example, when identification is performed using only one of these numbers:

- EI=0,25 (Negligible) when no other information is provided about the individual or it is not possible to find additional information unless access to the reference database is obtained
- EI=0,75 (Significant) when the identifier reveals additional identification information about the individual (e.g. social security number revealing date of birth) and is linked to other data (e.g. postal address or email).
- EI=1 (Maximum) when information from the reference database is also available (e.g. ID card and full name and/or picture).

Telephone number/Home address

They are both indirect identifiers, which can also be used to communicate with or access the individual. When identification is based only on one of these two identifiers:

- EI=0,25 (Negligible) throughout a country's population when the number/address is not registered in a publicly available register.
- EI=0,5 (Limited) throughout a small city's population and the number/address is not registered in a publicly available register (identification possible through communication).
- EI=1 (Maximum) throughout a country's population and the number/address is included in publicly available register.

Email address

It is also an indirect identifier, which can be used to communicate with the individual and in some cases it may include information about his/her name (first name and/or surname). When identification is based on email:

- EI=0,25 (Negligible) when the email address does not reveal any other identification information (e.g. name) and is not used as a primary address of the individual in internet sites, forums or social networks.
- EI=0,75 (Significant) when the email address does not reveal any other identification information (e.g. name) but is used as a primary address of the individual in internet sites, forums or social networks (searchable on the web).
- EI=1 (Maximum) when the email address reveals the individual's name and is used as his/her primary address in internet sites, forums or social networks (searchable on the web).

Picture

It may be a direct or indirect identifier, depending on the case. For example, when identification is based only on a picture:

- EI=0.25 (Negligible) when the picture is unclear or vague (e.g. CCTV footage from a long distance).
- EI=05 (Limited) when the picture is unclear or vague but it includes additional information (e.g. surroundings that show a specific location) that could lead to the identification of the individual.
- EI=0,75 (Significant) when the picture is clear but no other identification information is linked to it.
- EI=1 (Maximum) when the picture is clear and linked to some additional information (e.g. information about membership to a specific group, home address, etc).

Coding/Aliases/Initials

Coding refers to the assignment of a unique ID number to each individual, e.g. in the context of a specific database. The use of aliases is a form of pseudonymisation, in the sense that a specific identifier (usually the individual's full name) is substituted by an alias (pseudonym). The initials are a type of alias that is extracted from the full name of the individual. Like in the case of unique identifiers, codes and aliases can be used to identify the individual as long as it is possible to link them to a reference database (e.g. linking the code/alias to the full name of a particular person) When identification is based on coding or use of aliases:

- EI=0,25 (Negligible) when the code/alias does not reveal and cannot be linked to any other personal data about the individual unless access to the reference database is obtained.
- EI=0,75 (Significant) when the alias reveals some data about the individual (e.g. first name) and is linked to other personal data (e.g. the individual's email address).
- EI=1 (Maximum) when the alias reveals the individual's full name or data from the reference database are also available.

Annex 3 – Examples of the circumstances of the breach (CB) scoring

A1 Loss of confidentiality

0 – Examples of data exposed to confidentiality risks without evidence that illegal processing has occurred.

- ✓ A paper file or laptop is lost during transit.
- ✓ Equipment has been disposed without destruction of the personal data

+0.25 – Examples of data disposed to a number of known recipients:

- ✓ An email with personal data has been wrongly sent to a number of known recipients.
- ✓ Some customers could access other customers' accounts in an online service.

+0.5 – Examples of data disposed to an unknown number of recipients:

- ✓ Data are published on an internet message board.
- ✓ Data are uploaded to a P2P site.
- ✓ An employee sells a CD ROM with customer data.
- ✓ A wrongly configured website makes publically accessible on internet data from internal users.

A2 Loss of integrity

0 - Examples of data altered but without any identified incorrect or illegal use:

- ✓ The records of a database with personal data have been wrongly updated but the original has been obtained before any use of the altered data occurred.

+0.25 – Examples of data altered and possibly used in an incorrect or illegal way but with possibility to recover:

- ✓ A record that is necessary for the provision of an online social service has been changed and the individual needs to ask for the service in an offline way.
- ✓ A record that is important for the accuracy of an individual's file in an online medical service has been changed.

+0.5 – Examples of data altered and possibly used in an incorrect or illegal way without possibility to recover:

- ✓ The previous examples + the original cannot be recovered.

A3 Loss of availability

0 – Examples of data being recoverable without any difficulty:

- ✓ A copy of file is lost but other copies are available.
- ✓ A database is corrupted but can be easily reconstructed from other databases.

+0.25 – Examples of temporal unavailability:

- ✓ A database is corrupted but can be reconstructed from other databases, although some processing is required.
- ✓ A file is lost but the information can be provided again by the individual.

+0.5 – Examples of full unavailability (data cannot be recovered from the controller or the individuals):

- ✓ A file is lost/database corrupted, there is not back up of this information, and it cannot be provided by the individual.

A4 Malicious intent

+0.5 – The breach was due to an intentional action, e.g. in order to cause problem to the data controller (e.g. demonstrate loss of security) and/or in order to harm the individuals.

- ✓ An employee of a company intentionally shares private data from customers in a social media public site.
- ✓ An employee of a company sells private data from customers to another company.
- ✓ A member of a social network intentionally sends information about other members to their family members in order to harm them.

TP-04-13-118-EN-N

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

ISBN 978-92-9204-078-9
9 789292 040789
doi: 10.2824/27590

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

Procedura per la stima dell'impatto del Data Breach,
massimamente inspirata alla Procedura Enisa 2013, cui si rinvia nel caso di dubbi nella compilazione

Società/ Associazione/ Professionsita_
P.Iva_
Titolare o Responsabile?_
Ads_
Dpo_
Data compilazione_____

Breve descrizione del data Breach oggetto di verifica

All'esito della compilazione, il titolare è tenuto a fare copia del file EXCEL così come generato, associarlo alla riga del registro dei trattamenti e quindi marcarlo temporalmente.

Definzione dei dati personali oggetto del Data Breach			Per validare il dato mettere 1	
Genere	Specie	Punteggio	Moltiplicatore	Totale
Dati personali comuni (es: dati biografici, informazioni di contatto, nome e cognome, istruzuione, vita familiare, esperienze professionali)	**Punteggio preliminare di base** La violazione riguarda tale categoria di dati ed il titolare non è a conoscenza di alcun fattore di aggravamento	1	0	0
	Il volume dei dati personali comuni e/o le caratteristiche del titolare possono portare all'individuazione di status sociali e finanziari individuali	2	0	0
	I dati personali comuni e/o le caratteristiche del titolare possono portare all'individuazione diinformazioni afferenti alla salute, alle preferenze sessuali, all'apparetenza politica o alla fede religiosa	3	0	0
	A causa delle peculiari caratteristiche degli individui (es. appartenenza a minoranze) le informazioni possono rivelarsi critiche in relazione alla loro sicurezza personale o condizioni fisiche o psicologiche	4	0	0
			Subtot	0
Dati idonei a rivelare abitudini e/o comportamenti (Es. geolocalizzazione, dati del traffico telefonico/internet, preferenze personali, gusti ed abitudini, etc…)	**Punteggio preliminare di base** La violazione riguarda tale categoria di dati ed il titolare non è a conoscenza di alcun fattore di aggravamento o attenuazione	2	0	0
	La natura dei dati non è in grado di portare ad ulteriori informazioni legati a abitudini e/o comportamenti oppure tali dati possono essere raccolti con semplicità (indipendentemente dalla violazione) attraverso fonti pubbliche (es. ricerca web)	1	0	0
	Il volume di tali dati e/o le caratteristiche del titolare possono portare ad una profilazione dell'individuo , in grado di esporre dettagliate informazioni in relazione a le proprie abitudini quotidiane	3	0	0
	La violazione può portare alla creazione di un profilo individuale riferito a dati di natura sensibile	4	0	0
			Subtot	0

Dati finanziari (ogni tipo di dato finanziario -es. reddito, transazioni finanziarie, posizioni bancarie, investimenti, carte di credito, fatture, etc... - inclusi dati di sussidi statali collegati alle informazioni finanziarie	**Punteggio preliminare di base** La violazione riguarda tale categoria di dati ed il titolare non è a conoscenza di alcun fattore di aggravamento o attenuazione	3	0	0
	La natura dei dati non è in grado di portare ad ulteriori informazioni legate alle informazioni di natura finanziaria (es. il mero fatto che un individuo si cliente di una banca)	1	0	0
	I dati nello specifico includono informazioni di natura finanziaria ma non provvedono a fornire alcun significativo elemento circa lo status/situazione finanziaria dell'individuo (es. il numero di conto corrente senza uleriori dettagli)	2	0	0
	A causa della natura e/o del volume degli specifici dati, si rivelano informazioni finanziarie complete (es. relative ad una carta di credito) che possono condurre a frodi o alal creazione di un dettagliato profilo sociale/finanziario.	4	0	0
			Subtot	0
Dati sensibili (es. dati relativi alla salute, all'appartenenza politica, alla vita sessuale) e/o giudiziari	**Punteggio preliminare di base** La violazione riguarda tale categoria di dati ed il titolare non è a conoscenza di alcun fattore di attenuazione	4	0	0
	La natura dei dati non è in grado di portare ad ulteriori informazioni legati a abitudini e/o comportamenti oppure tali dati possono essere raccolti con semplicità (indipendentemente dalla violazione) attraverso fonti pubbliche (es. ricerca web)	1	0	0
	La natura dei dati può condurre a conclusioni di natura generica	2	0	0
	La natura dei dati può condurre a conclusioni circa informazioni di natura sensibile	3	0	0
			Subtot	0

Attenzione: nel caso in cui il Data Brach riguardi credenziali di accesso, dovrà farsi riferimento al tipo di dati che tali credenziali presidiano. Pertanto, a titolo di esempio, il furto di psw per accedere ad una cartella con dossier sanitari sarà da qualificarsi come furto di dati sensibili attinenti alla salute.

Totale DPC	0

(vale il subtotale maggiore)

	EI: Facilità di identificazione dell'interessato				
	Tipologia			Per validare il dato mettere 1	
1	NOME PER INTERO (Nome+ Cognome)	Semplicità nell'identificazione	Punteggio	Moltiplicatore	Totale
	Nome estremamente comune nella nazione individuata	Remota	0,25	0	0
	Nome poco comune nella nazione individuata	Debole	0,5	0	0
	Nome estramemente raro in una piccola città individuata	Significativa	0,75	0	0
	Il dato è associato a una data di nascita ed una mail	Massima	1	0	0
2	Carta idenità o altro documento identificativo			0	0
	Mancano ulteriori informazioni per eseguire associazione del dato	Remota	0,25	0	0
	Sussitono ulteriori informazioni che conducono ad ulteriori dati	Significativa	0,75	0	0
	Il dato è arrichito da informazioni univoche di contatto (foto, nome...)	Massima	1	0	0
3	Numero di telefono/ indirizzo di casa			0	0
	Il dato non è presente in alcun pubblico registro nazionale	Remota	0,25	0	0
	Il dato non è presente in alcun pubblico registro di una piccola città	Debole	0,5	0	0
	Il dato è presente in pubblici registri	Massima	1	0	0
4	Indirizzo mail			0	0
	L'indirizzo non rivela altre informazioni **ne** é associato a forum, siti, social...	Remota	0,25	0	0
	L'indirizzo non rivela altre informazioni **ma** é associato a forum, siti, social...	Significativa	0,75	0	0
	L'indirizzo rivela il nominativo del singolo **ed** é associato a forum, siti, social...	Massima	1	0	0
5	Immagine			0	0
	Immagine vaga e poco chiara (es. sfumata, distante...)	Remota	0,25	0	0
	Immagine vaga e poco chiara (es. sfumata, distante...) che tuttavia include ulteriori informazioni che possono condurre ad identificare il singolo)	Debole	0,5	0	0
	L'immagine è chiara ma non vi sono associate ulteriori informazioni	Significativa	0,75	0	0
	L'immagine è chiara e vi sono associate ulteriori informazioni	Massima	1	0	0
6	Codici/Alias/Iniziali			0	0
	Il dato non rivela né può essere associato ad altro dato personale senza l'accesso a database esterno	Remota	0,25	0	0
	Il dato è idoneo a rappresentare ulteriori informaizoni (es. mail) o altri dati personali (es. primo nome)	Significativa	0,75	0	0
	Il dato identifica il nome completo dell'interessato o è possibile accedere simultaneamente al database con cui effettuare l'associazione	Massima	1	0	0
				Totale EI	0
				Subtotale SE	0

	CBS: Circostanze della violazione (vd. Annex 3 Guida)			Per validare il dato mettere 1	
	Tipologia	Rilevanza	Punteggio	Moltiplicatore	
1	Violazione di riservatezza				
	La violazione della riservatezza non offre evidenza di azioni illecite (es. perdita di un pc durante una trasferta)	Remota	0	0	0
	Violazione della riservatezza con conoscenza dei soggetti non autorizzati alla conoscenza del dato (es. errore invio mail)	Debole	0,25	0	0
	Violazione della riservatezza senza conoscenza dei soggetti non autorizzati alla conoscenza del dato	Significativa	0,5	0	0
2	Violazione di integrità				0
	Dati alterati senza identificazioni scorrette o uso illecito dei dati (es. modifiche di un database senza sovrascrittura del precedente salvataggio)	Remota	0	0	0
	Dati alterati con possibili identificazioni scorrette o con possibile uso illecito dei dati ma con possibilità di ripristino degli stessi	Debole	0,25	0	0
	Dati alterati senza possibili identificazioni scorrette o con possibile uso illecito dei dati ma con possibilità di ripristino degli stessi	Significativa	0,5	0	0
3	Violazione di disponibilità				0
	Dati persi ma facilmente recuperabili	Remota	0	0	0
	La perdita dei dati comporta la non disponibilità degli stessi per un certo periodo di tempo	Debole	0,25	0	0
	La perdita dei dati è irreversibile	Significativa	0,5	0	0
4	Data Breach a seguito di azione dolosa di terzi diversi dal titolare				0
	In qualunque modo accada, è sempre evento significativo	Significativa	0,5	0	0

Annotazioni finali_

Totale CSBS	0
Risultato finale Data Breach Assessment	0

			Ulteriori fattori (mettere x)	
			Impatto sul larga scala (>100)	Indecifrabilità dei dati
Risultato	Se Risultato <2	Impatto basso		
	Se 2 ≤ Risultato <3	Impatto medio		
	Se 3 ≤ Risultato <4	Impatto significativo		
	Se4 ≤ Risultato	Impatto estremamente significativo		
			Impatto aumentato	Impatto ridotto

	Registro Data Braches azienda_________					
	Data Della Violazione	Breve descrizione dell'incidente	Circostanze	Conseguenze stimate per i diritti degli interessati	Provvedimenti adottati	Motivazione alla base del provvedimento adottato

INDIRIZZI E LINEE GUIDA DI ADATTAMENTO DEL MODELLO ORGANIZZATIVO DEL COMUNE DI ANGUILLARA VENETA AL D.LGS. N. 101/2018 IN MATERIA DI TRATTAMENTO DEI DATI DI RECEPIMENTO DEL REGOLAMENTO (UE) 2016/679.

Art. 1
Oggetto e ambito di applicazione

a) **Il Comune di Anguillara Veneta** è il **titolare del trattamento dei dati personali**;
b) La presente delibera individua i soggetti medianti i quali il **Comune di Anguillara Veneta** esercita le funzioni di **titolare del trattamento dei dati personali**;
c) Le disposizioni della presente delibera si applicano a tutte le strutture organizzative (Uffici) del **Comune di Anguillara Veneta**.

Art. 2
Esercizio delle funzioni di titolare del trattamento dei dati personali

In conformità' all'assetto organizzativo del Comune di Anguillara Veneta, nell'ambito delle strutture di cui all'art. 1, comma c), i soggetti individuati per l'esercizio delle funzioni **di titolare del trattamento dei dati personali**, ciascuno nel rispettivo ambito di competenza, sono tutti i **Responsabili di Servizio (titolari di P.O.).**

Art. 3
Le competenze del "Titolare del trattamento dei dati personali"

Al **Titolare** di cui all'art. 4 par. 1 punto 7) del Regolamento (UE) 2016/679 sono riconducibili le seguenti principali competenze:

a) determina le finalità e i mezzi del trattamento dei dati personali: è la funzione fondamentale che riassume e ordina tutte le altre (art. 4);

b) in caso di minori, verifica che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale (art. 9);

c) agevola l'esercizio dei diritti dell'interessato (art. 12) e fornisce agli interessati le informazioni indicate dal GDPR (art. 13);

d) mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento: è il principio di responsabilizzazione (accountability), perno di tutto il GDPR (art. 24);

e) individua i responsabili del trattamento e ne controlla e garantisce l'operato (art. 28);

f) tiene un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);

g) garantisce l'idonea formazione del personale incaricato del trattamento (art. 32);

h) comunica all'autorità di controllo (art. 33) e all'interessato (art. 34) eventuali violazioni dei dati;

i) effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35);

l) designa il responsabile della protezione dei dati (DPO - art. 37) mettendolo in grado di svolgere adeguatamente l'attività (art. 38);

m) è destinatario di provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);

n) risponde per il danno cagionato dal suo trattamento che violi il presente regolamento (art. 82);

o) è destinatario delle sanzioni amministrative pecuniarie inflitte ai sensi del GDPR (art. 83).

Art. 4
Attribuzioni delle competenze del titolare

Le competenze sopra elencate e le altre previste nel GDPR sono attribuite agli organi del comune in relazione alle funzioni agli stessi assegnati dalla Legge n. 56/2014, dal D.Lgs. n. 267/2000 e dallo statuto comunale:

1. al **consiglio comunale** sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;

2. all'**organo esecutivo (**Giunta comunale**)** sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo;

3. all'**organo di vertice** (sindaco) competono le nomine, con riferimento in particolare ai responsabili interni del trattamento e al responsabile della protezione dei dati;

4. ai **Responsabili del servizio,** in qualità di **titolar**i, secondo l'ambito di competenza, spettano i seguenti compiti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

b) disporre, in conseguenza alla verifica di cui alla lett. a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

c) adottare soluzioni di privacy by design e by default;

d) contribuire al costante aggiornamento del registro delle attività di trattamento;

e) garantire la corretta informazione e l'esercizio dei diritti degli interessati;

f) individuare responsabili del trattamento e i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;

g) disporre l'adozione dei provvedimenti imposti dal Garante;

h) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

i) adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri dirigenti, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;

l) individuare, negli atti di costituzione di eventuali gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;

m) garantire al DPO e al personale designato amministratore di sistema del Comune i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

n) la preventiva valutazione d'impatto, ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

o) consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1, lett b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35, indichi che il trattamento presenta un rischio residuale elevato;

p) individuare i responsabili esterni del trattamento fornendo le necessarie indicazioni.

Art. 5
I designati al trattamento

Per tutti i compiti non svolti in quanto titolare, ogni responsabile del servizio è individuato quale **designato del trattamento dei dati personali** relativamente ai servizi e uffici di competenza, in forza dell'incarico di titolare di posizione organizzativa e senza necessita di atti ulteriori. Gli atti di incarico di titolare di posizione organizzativa riportano, sinteticamente gli elementi di cui all'art. 28 del Regolamento.

Art. 6
I responsabili esterni al trattamento

Sono designati responsabili esterni del trattamento di dati personali i soggetti estranei all'amministrazione comunale che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare. Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Art. 7
Autorizzazione al trattamento

I dipendenti dell'ente a tempo determinato o indeterminato sono **autorizzati** al compimento alle operazioni di **trattamento dei dati** in forza del contratto di lavoro e dell'inserimento nella struttura organizzativa dell'ente, limitatamente ai trattamenti di competenza del servizio/ufficio di appartenenza.
I responsabili del servizio in qualità di titolari ne curano la formazione in materia di trattamento dei dati e forniscono le necessarie istruzioni, verificandone l'applicazione.
I collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare sono autorizzati al trattamento dati mediante espressa attribuzione nel contratto di incarico. La designazione scritta deve inoltre contenere, quando necessarie, le istruzioni specifiche non già contenute nelle istruzioni generali impartite al personale dipendente o inserito ad altro titolo.

INDIRIZZI E LINEE GUIDA DI ADATTAMENTO DEL MODELLO ORGANIZZATIVO DEL COMUNE DI ANGUILLARA VENETA AL D.LGS. N. 101/2018 IN MATERIA DI TRATTAMENTO DEI DATI DI RECEPIMENTO DEL REGOLAMENTO (UE) 2016/679.

Art. 1
Oggetto e ambito di applicazione

a) **Il Comune di Anguillara Veneta** è il **titolare del trattamento dei dati personali**;
b) La presente delibera individua i soggetti medianti i quali il **Comune di Anguillara Veneta** esercita le funzioni di **titolare del trattamento dei dati personali**;
c) Le disposizioni della presente delibera si applicano a tutte le strutture organizzative (Uffici) del **Comune di Anguillara Veneta**.

Art. 2
Esercizio delle funzioni di titolare del trattamento dei dati personali

In conformità' all'assetto organizzativo del Comune di Anguillara Veneta, nell'ambito delle strutture di cui all'art. 1, comma c), i soggetti individuati per l'esercizio delle funzioni **di titolare del trattamento dei dati personali**, ciascuno nel rispettivo ambito di competenza, sono tutti i **Responsabili di Servizio (titolari di P.O.).**

Art. 3
Le competenze del "Titolare del trattamento dei dati personali"

Al **Titolare** di cui all'art. 4 par. 1 punto 7) del Regolamento (UE) 2016/679 sono riconducibili le seguenti principali competenze:

a) determina le finalità e i mezzi del trattamento dei dati personali: è la funzione fondamentale che riassume e ordina tutte le altre (art. 4);

b) in caso di minori, verifica che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale (art. 9);

c) agevola l'esercizio dei diritti dell'interessato (art. 12) e fornisce agli interessati le informazioni indicate dal GDPR (art. 13);

d) mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento: è il principio di responsabilizzazione (accountability), perno di tutto il GDPR (art. 24);

e) individua i responsabili del trattamento e ne controlla e garantisce l'operato (art. 28);

f) tiene un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);

g) garantisce l'idonea formazione del personale incaricato del trattamento (art. 32);

h) comunica all'autorità di controllo (art. 33) e all'interessato (art. 34) eventuali violazioni dei dati;

i) effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35);

l) designa il responsabile della protezione dei dati (DPO - art. 37) mettendolo in grado di svolgere adeguatamente l'attività (art. 38);

m) è destinatario di provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);

n) risponde per il danno cagionato dal suo trattamento che violi il presente regolamento (art. 82);

o) è destinatario delle sanzioni amministrative pecuniarie inflitte ai sensi del GDPR (art. 83).

Art. 4
Attribuzioni delle competenze del titolare

Le competenze sopra elencate e le altre previste nel GDPR sono attribuite agli organi del comune in relazione alle funzioni agli stessi assegnati dalla Legge n. 56/2014, dal D.Lgs. n. 267/2000 e dallo statuto comunale:

1. al **consiglio comunale** sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;

2. all'**organo esecutivo (**Giunta comunale**)** sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo;

3. all'**organo di vertice** (sindaco) competono le nomine, con riferimento in particolare ai responsabili interni del trattamento e al responsabile della protezione dei dati;

4. ai **Responsabili del servizio,** in qualità di **titolar**i, secondo l'ambito di competenza, spettano i seguenti compiti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;

b) disporre, in conseguenza alla verifica di cui alla lett. a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;

c) adottare soluzioni di privacy by design e by default;

d) contribuire al costante aggiornamento del registro delle attività di trattamento;

e) garantire la corretta informazione e l'esercizio dei diritti degli interessati;

f) individuare responsabili del trattamento e i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;

g) disporre l'adozione dei provvedimenti imposti dal Garante;

h) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

i) adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri dirigenti, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;

l) individuare, negli atti di costituzione di eventuali gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;

m) garantire al DPO e al personale designato amministratore di sistema del Comune i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;

n) la preventiva valutazione d'impatto, ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

o) consultare il Garante, in aderenza all'art. 36 del Regolamento e nelle modalità previste dal par. 3.1, lett b), nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35, indichi che il trattamento presenta un rischio residuale elevato;

p) individuare i responsabili esterni del trattamento fornendo le necessarie indicazioni.

Art. 5
I designati al trattamento

Per tutti i compiti non svolti in quanto titolare, ogni responsabile del servizio è individuato quale **designato del trattamento dei dati personali** relativamente ai servizi e uffici di competenza, in forza dell'incarico di titolare di posizione organizzativa e senza necessita di atti ulteriori. Gli atti di incarico di titolare di posizione organizzativa riportano, sinteticamente gli elementi di cui all'art. 28 del Regolamento.

Art. 6
I responsabili esterni al trattamento

Sono designati responsabili esterni del trattamento di dati personali i soggetti estranei all'amministrazione comunale che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare. Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Art. 7
Autorizzazione al trattamento

I dipendenti dell'ente a tempo determinato o indeterminato sono **autorizzati** al compimento alle operazioni di **trattamento dei dati** in forza del contratto di lavoro e dell'inserimento nella struttura organizzativa dell'ente, limitatamente ai trattamenti di competenza del servizio/ufficio di appartenenza.
I responsabili del servizio in qualità di titolari ne curano la formazione in materia di trattamento dei dati e forniscono le necessarie istruzioni, verificandone l'applicazione.
I collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare sono autorizzati al trattamento dati mediante espressa attribuzione nel contratto di incarico. La designazione scritta deve inoltre contenere, quando necessarie, le istruzioni specifiche non già contenute nelle istruzioni generali impartite al personale dipendente o inserito ad altro titolo.

Allegato Sub. B) alla delibera di G.C. n. 91 **del** 31/10/2019

REGISTRO DELLE ATTIVITA' DEL TITOLARE DEL TRATTAMENTO

Comune di Anguillara Veneta

Introduzione

Il registro dei trattamenti è un documento che censisce le caratteristiche principali dell'attività del titolare del trattamento. La sua funzione è prevalentemente descrittiva e il suo contenuto deve corrispondere alla realtà dei fatti. Esso costituisce la base per eseguire gli ulteriori adempimenti (informative, nomine soggetti autorizzati, ecc.).

I soggetti tenuti alla redazione del registro dei trattamenti sono individuati dall'art. 30 Reg UE 2016/679

Per i Comuni, quale quello di Anguillara Veneta, la predisposizione del registro delle attività di trattamento è prevista dal GDPR.

Il Garante sottolinea inoltre che, a prescindere dall'obbligo normativo, è essenziale predisporre la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro.

Conformemente a quanto imposto dall'art. 30 del Regolamento ed alle sopracitate premesse, il presente registro indicherà, in relazione ad ogni trattamento:

- ✓ Il nome e i dati di contatto del Titolare del Trattamento e del Responsabile per la Protezione dei Dati (RPD/DPO);
- ✓ Le finalità del trattamento;
- ✓ Le categorie di interessati e le categorie di dati trattati;
- ✓ Le categorie di destinatari ai quali vengono comunicati i dati;
- ✓ Eventuali trasferimenti di dati verso paesi extra-UE od organizzazioni internazionali;
- ✓ Dopo l'elencazione dei trattamenti, ove applicabile, la tabella indicante i termini di conservazione dei dati per ogni categoria di interessato e ogni categoria di dato;
- ✓ Una descrizione degli asset (strumenti e risorse) coinvolti nel trattamento e le relative misure di sicurezza tecniche e organizzative applicate.

Registro delle attività del Titolare del Trattamento

Ai sensi dell'art. 30.1 Reg. UE 2016/679

Valutazione e misurazione delle performance dei dipendenti

Descrizione: Il trattamento in oggetto riguarda il sistema di misurazione e valutazione delle performance organizzative ed individuali dei dipendenti del comune ex Dgls 150/2009 e s.m.i., in ossequio alla Delibera Comunale.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Valutazione delle prestazioni del personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.lgs. 150/2009 Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività' del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Dipendenti	Ruolo ricoperto in azienda Curriculum Vitae Dati relativi alla qualità della prestazione lavorativa Buste paga Dati di contatto (numero di telefono, e-mail, ecc.)		

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Dipendenti	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice Responsabili	Descrizione
Asset fisici	Personal Computer	PCA	Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Information asset	Cartella dipendenti	CD1	Cartella contenente i dati del personale dipendente
Information asset	Archivio personale	AP	Archivio cartaceo dei dati relativi al personale e/o collaboratori esterni dell'Ente
Risorse IT	Server	SBB	Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Cartella dipendenti	CD1	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Sistema di gestione degli accessi alla cartella	
Archivio personale	AP	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Contenitori con chiave	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	

Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Servizi demografici / Anagrafe - gestione dell'anagrafe della popolazione residente e dell'anagrafe della popolazione residente all'estero (AIRE)

Descrizione: Indipendentemente dall'alto numero di dati contenuti negli archivi anagrafici, quelli di carattere "sensibile" concernono solo le informazioni sull'origine razziale, in quanto tali idonei a rivelare le convinzioni religiose, inseriti negli anni 1938-44 in virtù delle "leggi razziali"; questi dati, che sono idonei a rivelare in taluni casi anche le convinzioni religiose, non sono comunque resi noti (art. 3, r.d.l. n. 25/1944); le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere altresì presenti dati sulle patologie pregresse, in considerazione del fatto che fino al 1968 le schede anagrafiche riportavano le cause di decesso.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Tenuta delle anagrafi della popolazione residente in Italia e di cittadini italiani residenti all'estero	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini		Dati personali idonei a rivelare lo stato di salute Dati idonei a rivelare le convinzioni religiose Dati personali idonei a rivelare la vita sessuale	Dati relativi ad altri provvedimenti o procedimenti giudiziari

Dati idonei a rivelare l'origine razziale
ed etnica

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	

Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Attività di segreteria generale

Descrizione: Il trattamento riguarda i compiti che sono assegnati all'Ufficio dalla legge, dal regolamento sull'ordinamento degli uffici e dei servizi, e dal Sindaco. L'ufficio assiste inoltre gli organi di governo dell'ente nell'azione amministrativa assicurando il rispetto della legittimità dei provvedimenti.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa alla tenuta del repertorio, rogito, registrazione e trascrizione dei contratti e atti unilaterali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000, art. 97, comma 4, lettera c)
Attività di Centralino	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000, art. 13, comma 1.
Accoglimento dei visitatori	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000, art. 13, comma 1
Gestione contributi comunali su mutui prima casa	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000, art. 13, comma 1
Gestione degli adempimenti in materia di Anticorruzione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Legge n. 190/2012.

Gestione dei dati relativi agli organi istituzionali dell'ente, dei difensori civici, nonché dei rappresentanti dell'ente presso enti, aziende e istituzioni	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento d.lgs. n. 267/2000, Titolo III°, capo I°
Attività di rappresentanza comune	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento d.lgs. n. 267/2000, Titolo III°, capo I°
Attività di individuazione del miglior contraente	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento D.lgs. n. 50/2016
Attività di supporto al personale amminsitrativo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento d.lgs. n. 267/2000, Titolo III°, capo I°
Gestione degli adempimenti in materia di Trasparenza della P.A.	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento D.Lgs. n. 33/2013
Attività di direzione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento .lgs. n. 267/2000, Titolo IV°, Capo iii°
Attività di controllo sulla completezza e correttezza dei documenti	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento Legge n. 241/1990
Attività di stipula dei contratti in nome e per conto dell'ente	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento d.lgs. n. 267/2000, art. 97, comma 4, lettera c)

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Dati relativi alla situazione reddituale		Dati relativi ai carichi pendenti e al casellario giudiziale
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica

Soggetti a qualunque titolo interessati da rapporti con l'Ente	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	

Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Servizi demografici / Stato civile - Attività di gestione dei registri di stato civile

Descrizione: Indipendentemente dall'alto numero di dati contenuti negli archivi anagrafici, quelli di carattere "sensibile" sono quelli concernenti l'origine razziale, in quanto tali idonei a rivelare le convinzioni religiose, inseriti negli anni 1938-44 in virtù delle "leggi razziali"; questi dati, che sono idonei a rivelare in taluni casi anche le convinzioni religiose, non sono comunque resi noti (art. 3, r.d.l. n. 25/1944); ulteriori informazioni sull'origine razziale o etnica possono essere desunte dagli atti relativi alle adozioni internazionali. Altri dati sensibili contenuti in tali archivi possono essere raccolti anche da terzi e comunicati all'Autorità giudiziaria per le cause di interdizione e decesso, alla ASL per l'aggiornamento del registro delle cause di morte. Vengono altresì trattati dati di carattere giudiziario; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso
.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Tenuta degli atti e dei registri dello stato civile	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati idonei a rivelare le convinzioni religiose	

Stato di salute - patologie attuali

Dati personali idonei a rivelare la vita sessuale

Stato di salute - patologie pregresse

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	ASL

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna Lock postazione	

		Virus (malware)	Firewall
			Antivirus
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Servizi demografici / Elettorale - attività relativa alla tenuta dell'elenco dei giudici popolari

Descrizione: I dati vengono forniti dall'interessato, che presenta una domanda contenente il titolo di studio e la professione, oppure vengono estratti casualmente dalle liste elettorali; vengono controllati i requisiti prescritti dalla legge e richieste le certificazioni necessarie anche a terzi. Viene quindi formato l'elenco provvisorio che è trasmesso al Tribunale; quest'ultimo procede ad una verifica sui carichi pendenti e restituisce l'elenco al Comune per la pubblicazione e la formazione dell'elenco definitivo.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa alla tenuta dell'elenco dei giudici popolari	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.
	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		Dati relativi ai carichi pendenti e al casellario giudiziale Dati relativi ad altri provvedimenti o procedimenti giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Amministrazioni dello Stato

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi demografici / Elettorale - attività relativa all'elettorato attivo e passivo

Descrizione: Tenuta lista elettorali ed operazione connesse.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa all'elettorato attivo e passivo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Iscritti o candidati a partiti politici o liste civiche	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati idonei a rivelare l'adesione a partiti	
Cittadini			

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Iscritti o candidati a partiti politici o liste civiche	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato
Cittadini	

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Iscritti o candidati a partiti politici o liste civiche	Altre amministrazioni ed enti pubblici
Cittadini	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi demografici / Elettorale - attività relativa alla tenuta degli albi degli scrutatori e dei presidenti di seggio

Descrizione: I dati vengono forniti dall'interessato; la commissione elettorale comunale procede ad un'estrazione pubblica dei componenti del seggio; vengono confrontati con le liste di leva per la verifica del diritto al voto; vengono stampate le notifiche per gli scrutatori e redatti i verbali delle nomine. I dati sulla salute si riferiscono esclusivamente a quelli rinvenibili nei certificati medici che gli scrutatori sono tenuti a presentare in caso di indisponibilità per motivi di salute.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica

Richieste di referendum, relative consultazioni e verifica della regolarità	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.
Svolgimento delle consultazioni elettorali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti interessati allo svolgimento delle consultazioni elettorali		Stato di salute - patologie attuali	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti interessati allo svolgimento delle consultazioni elettorali	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Soggetti interessati allo svolgimento delle consultazioni elettorali	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti interessati allo svolgimento delle consultazioni elettorali	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi demografici / Leva - attività relativa alla tenuta delle liste di leva e dei registri matricolari

Descrizione: Il procedimento inizia con la formazione della lista di leva del Comune stesso e la successiva comunicazione dei soggetti iscritti nelle liste di leva al Distretto militare, quindi vengono costituite le liste di leva ed i registri dei ruoli matricolari. L'Ufficio leva riceve dal distretto militare, le comunicazioni relative agli iscritti di leva dichiarati renitenti, rivedibili e riformati dalle competenti autorità militari al fine di effettuare le pertinenti annotazioni sulla lista di leva e sui registri dei ruoli matricolari, nonché per procedere all'adozione di determinazioni ministeriali concernenti i nominativi dei soggetti dichiarati espulsi dall'esercito, cancellati dai ruoli matricolari, ecc.. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. I dati vengono comunicati al

Distretto militare di appartenenza al fine di consentire l'effettuazione delle procedure di arruolamento.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa alla tenuta delle liste di leva e dei registri matricolari	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	**Categorie Particolari di Dati ex art. 9**	**Categorie relativi a condanne penali e reati ex art. 10**
Cittadini		Stato di salute - patologie attuali Stato di salute - terapie in corso Stato di salute - patologie pregresse	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Gestione contributi e patrocinii eventi sportivi

Descrizione: Il patrocinio costituisce il riconoscimento da parte del Comune delle iniziative promosse da Enti, Associazioni, organizzazioni pubbliche e private, di particolare valore sportivo (nel caso di specie). Il patrocinio può essere: oneroso e non oneroso.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività sportive	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Rappresentanti e/o iscritti ad enti o associazioni senza scopo di lucro	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	
		Dati idonei a rivelare lo stato di gravidanza	
Soggetti minorenni	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati idonei a rivelare lo stato di disabilità	
	Dati idonei a rivelare il rapporto di parentela	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Rappresentanti e/o iscritti ad enti o associazioni senza scopo di lucro	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1
Soggetti minorenni	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Rappresentanti e/o iscritti ad enti o associazioni senza scopo di lucro	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati
Soggetti minorenni	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Information asset	Cartella contabilità	CC		Cartella contenente i dati relativi alla contabilità
Information asset	Archivio contabilità	AC		Archivio cartaceo contenente dati di ospiti, fornitori, consulenti, dipendenti relativi alla contabilità dell'ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Cartella contabilità	CC	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Sistema di gestione degli accessi alla cartella	

Archivio contabilità	AC	Trattamento (volontario o inconsapevole) non consentito di dati (personali)		Contenitori con chiave
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Economato, Tributi ed entrate comunali

Descrizione: Il servizio si occupa degli aspetti amministrativo-contabili di gestione dell'ente, compresa la gestione dei tributi locali.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Gestione tributi ed entrate comunali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000,Titolo III°, Capo I°
Gestione delle procedure sanzionatorie	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000,Titolo III°, Capo I°
Attività relative al recupero evasione tributaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	d.lgs. n. 267/2000,Titolo III°, Capo I°

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10

Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Information asset	Cartella contabilità	CC		Cartella contenente i dati relativi alla contabilità
Information asset	Archivio contabilità	AC		Archivio cartaceo contenente dati di ospiti, fornitori, consulenti, dipendenti relativi alla contabilità dell'ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Cartella contabilità	CC	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Sistema di gestione degli accessi alla cartella	

Archivio contabilità	AC	Trattamento (volontario o inconsapevole) non consentito di dati (personali)		Contenitori con chiave
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Controlli edilizi

Descrizione: L'Ufficio svolge attività di: - Controlli edilizi, esame dei rapporti dei Vigili Urbani, sopralluoghi vari e attività amministrativa e sanzionatoria connessa (predisposizione di ordinanze di sospensione dei lavori, di demolizione, adozione delle misure sanzionatorie per lavori abusivi etc.); - Ordinanze contingibili e urgenti in materia edilizia; - Esercizio di attività di consulenza nei confronti degli Organi del Comune per quanto attiene alle materie di competenza; - Verifiche per idoneità all'alloggio.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.P.R. n. 380/2001
Attività di verifica del rispetto della normativa di settore	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.P.R. n. 380/2001

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10

Imprenditori	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati giudiziari
Lavoratori autonomi	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati giudiziari
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati giudiziari
Soggetti richiedenti licenze o autorizzazioni amministrative	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati giudiziari

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Imprenditori	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001
Lavoratori autonomi	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001
Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001
Soggetti richiedenti licenze o autorizzazioni amministrative	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Imprenditori	Altre amministrazioni ed enti pubblici
Lavoratori autonomi	Altre amministrazioni ed enti pubblici
Cittadini	Altre amministrazioni ed enti pubblici
Soggetti richiedenti licenze o autorizzazioni amministrative	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Urbanistica ed edilizia

Descrizione: L'area si occupa della tenuta e della gestione del Piano regolatore generale, degli strumenti urbanistici esecutivi, e di tutti gli atti di pianificazione territoriale. Rilascia i titoli a costruire, si interessa dell'agibilità delle costruzioni, certifica le destinazioni urbanistiche dei terreni, ed è l'ufficio destinatario a cui inoltrare i fascicoli edilizi.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281

	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Gestione delle pratiche relative ai progetti edilizi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali; D.P.R. 380/2001
Gestione delle pratiche connesse all'abbattimento delle barriere architettoniche e all'agibilità di percorsi ed edifici	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001
Gestione delle pratiche relative alle istruttorie in materia urbanistica	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001
Gestione introiti oneri urbanizzazione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001
Gestione delle pratiche relative ai permessi di costruire	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.P.R. 380/2001

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		
Soggetti richiedenti licenze o autorizzazioni amministrative	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici
Soggetti richiedenti licenze o autorizzazioni amministrative	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Rilascio delle licenze per il commercio, il pubblico esercizio, l'artigianato e la pubblica sicurezza

Descrizione: I dati giudiziari vengono acquisiti ed istruiti a seguito di presentazione di domanda da parte di persone fisiche o giuridiche, nonché acquisiti dal casellario giudiziario e vengono trattati nell'ambito del procedimento per il rilascio di licenze, autorizzazioni e analoghi provvedimenti.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa al rilascio di licenze, autorizzazioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 114/2018; legge 287/1991; legge 443/1985; TULPS RD 773/1931

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Imprenditori	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		Dati giudiziari
Commercianti	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		Dati giudiziari

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Imprenditori	Trattamento dei dati personali relativi a condanne penali e reati. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 114/2018; legge 287/1991; legge 443/1985; TULPS RD 773/1931

Commercianti	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 114/2018; legge 287/1991; legge 443/1985; TULPS RD 773/1931

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Imprenditori	Altre amministrazioni ed enti pubblici
Commercianti	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	

Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Polizia Municipale- attività di polizia giudiziria e di pubblica sicurezza

Descrizione: Il trattamento riguarda le attività di polizia locale inerenti a servizio di prevenzione, controllo e vigilanza sull'osservanza delle norme, delle regole e dei comportamenti, nonché delle funzioni di polizia giudiziaria, ovvero l'investigazione in autonomia fino a che il PM, interessato della notizia di reato, non abbia assunto la direzione delle indagini impartendo le relative istruzioni (art. 348 cpp),

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di polizia giudiziaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali; Legge 65/1986; TULPS RD 773/1931
Attività di pubblica sicurezza	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali; Legge 65/1986; TULPS RD 773/1931

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati personali idonei a rivelare lo stato di salute Dati personali idonei a rivelare la vita sessuale	Dati giudiziari

Dati idonei a rivelare l'origine nazionale

Dati idonei a rivelare l'origine razziale ed etnica

Dati idonei a rivelare caratteristiche o idoneità psico-fisiche

Impronte digitali

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti a qualunque titolo interessati da rapporti con l'Ente	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali Legge 65/1986; TULPS RD 773/1931

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Attività di polizia protezione civile

Descrizione: Ufficio di coordinamento tra l'attività della protezione civile e la polizia locale per garantire l'esecuzione degli obblighi e delle attività necessarie nelle situazioni emergenziali.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali; D.lgs. 1/2018

Attività di pubblica sicurezza	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali; D.lgs. 1/2018

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio) Dati di contatto (numero di telefono, e-mail, ecc.)		

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna Lock postazione	

		Virus (malware)	Firewall
			Antivirus
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Polizia municipale - Attività relativa all'infortunistica stradale

Descrizione: I dati vengono acquisiti in occasione della rilevazione di incidenti e/o infortuni; gli stessi servono per l'individuazione delle persone coinvolte e l'accertamento dei fatti. Vengono verbalizzati i fatti e contestate le eventuali sanzioni amministrative ed in caso di illeciti penali, o che comportino provvedimenti sui permessi di guida, i dati rilevati sono trasmessi agli enti competenti (Dipartimento per i trasporti terrestri, Prefettura)

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di polizia amministrativa	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986;

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10

Soggetti coinvolti in incidenti e/o infortuni stradali	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Stato di salute - patologie attuali Stato di salute - terapie in corso

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti coinvolti in incidenti e/o infortuni stradali	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Soggetti coinvolti in incidenti e/o infortuni stradali	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986;

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti coinvolti in incidenti e/o infortuni stradali	Dipartimento per i trasporti terrestri e Prefettura Familiari Assicurazioni

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Polizia municipale - Gestione delle procedure sanzionatorie

Descrizione: I dati vengono acquisiti tramite i verbali elevati da enti e Forze dell'ordine e/o ispezioni effettuate dagli organi addetti al controllo; tuttavia essi possono essere reperiti anche direttamente dagli interessati, qualora gli stessi presentino dei ricorsi.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Gestione delle procedure sanzionatorie		Legge 65/1986; Legge 689/1981

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini		Stato di salute - patologie attuali Stato di salute - relativo a familiari Stato di salute - terapie in corso Stato di salute - patologie pregresse	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986; Legge 689/1981.

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Dipartimento per i trasporti terrestri e Prefettura

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Polizia municipale - Attività di polizia annonaria, commerciale ed amministrativa

Descrizione: I dati (in particolare quelli contenuti nel c.d. "certificato antimafia") vengono acquisiti dagli interessati al momento della presentazione delle domande per le licenze o per le autorizzazioni amministrative; gli stessi vengono poi esaminati al fine di verificare l'esistenza dei requisiti richiesti. I dati sulla salute vengono trattati, in particolare, al fine di verificare i requisiti richiesti nel caso di soggetti preposti alla gestione di determinate attività, come ad esempio la rivendita di generi alimentari. I dati possono essere anche acquisiti attraverso i controlli svolti presso l'esercizio o l'attività dell'interessato, al fine di verificare le autorizzazioni e la relativa regolarità; in tal caso viene redatto un verbale di ispezione, cui segue una verifica presso gli uffici comunali competenti
.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281

	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di polizia amministrativa locale, con particolare riferimento ai servizi di igiene	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986; D.Lgs. 159/2011

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti coinvolti in violazioni in materia sanitaria o ambientale	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Stato di salute - patologie attuali	Dati giudiziari
Cittadini	Dati di contatto (numero di telefono, e-mail, ecc.)	Stato di salute - patologie attuali	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti coinvolti in violazioni in materia sanitaria o ambientale	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali
Cittadini	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Soggetti coinvolti in violazioni in materia sanitaria o ambientale	Trattamento dei dati personali relativi a condanne penali e reati. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986; D.Lgs. 159/2011

	tenuto soltanto sotto il controllo dell'autorità pubblica	
Cittadini	Trattamento dei dati personali relativi a condanne penali e reati. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986; D.Lgs. 159/2011

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti coinvolti in violazioni in materia sanitaria o ambientale	Altre amministrazioni ed enti pubblici
Cittadini	Amministrazioni dello Stato

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	

Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Polizia municipale - Attività relativa al rilascio di permessi per invalidi

Descrizione: I dati vengono acquisiti attraverso la domanda presentata dall'interessato, che contiene anche il certificato del medico legale. I dati vengono inoltre comunicati all'Autorità giudiziaria e a quella di pubblica sicurezza con riferimento ai soggetti disabili coinvolti in indagini di polizia giudiziaria per contraffazione e/o duplicazione del contrassegno rilasciato dall'Amministrazione comunale, nonché alle A.S.L., che provvedono a fornire le necessarie informazioni per l'accertamento dell'invalidità dell'interessato. In seguito all'esame della richiesta, si procede ad adottare una decisione relativamente alla possibilità di rilasciare o meno il permesso.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di polizia amministrativa	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Legge 65/1986; D.P.R. 151/2012; Legge 35/2012; Legge 104/1992

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti portatori di handicap		Stato di salute - patologie attuali	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti portatori di handicap	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti portatori di handicap	Autorità giudiziaria
	ASL

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	

Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Polizia municipale - Attività di vigilanza edilizia, in materia di ambiente e sanità, nonché di polizia mortuaria

Descrizione: I dati giudiziari e sulla salute vengono acquisiti attraverso i controlli svolti sul territorio, che sono effettuati su iniziativa d'ufficio, ovvero su richiesta di privati, di enti e di associazioni; oltre alla verifica in loco, vengono avviati i necessari accertamenti presso gli uffici competenti, al termine dei quali viene predisposta una relazione finale con l'indicazione delle eventuali violazioni in materia sanitaria o ambientale riscontrate. In tal caso, si procede a trasmetterle alle competenti autorità amministrative o penali. Vengono, inoltre, effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. Per quanto concerne l'attività di polizia mortuaria, ed i connessi servizi cimiteriali, i dati vengono forniti direttamente dagli interessati, dai familiari o dal rappresentante della comunità religiosa, che presentano apposita domanda al Comune al fine di ottenere delle particolari forme di sepoltura. I dati sulla salute vengono trattati in quanto i medici debbono denunciare al sindaco la malattia che, a loro giudizio, sarebbe stata la causa di morte di persona da loro assistita. Il comune a sua volta comunica le cause di morte all'ISTAT per le rilevazioni annuali, nonché alla ASL competente per territorio per l'aggiornamento del registro delle cause di morte
.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di polizia amministrativa locale, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 65/1986; D.P.R. 380/2001; R.D. 1265/1934; D.Lgs. 152/2006; D.P.R. 285/1990

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati idonei a rivelare le convinzioni religiose Stato di salute - patologie attuali	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Ente gestore degli alloggi mortuari (per l'erogazione del servizio) ISTAT ASL

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al	

			trattamento e mediante specifica policy interna
			Lock postazione
		Virus (malware)	Firewall
			Antivirus
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Servizi sociali - Attività relativa all'assistenza domiciliare

Descrizione: I dati vengono forniti direttamente dagli interessati, i quali presentano apposita domanda al Comune ovvero da terzi (Polizia municipale e Forze di polizia; INPS, ASL, azienda ospedaliera, IPAB, medici di base; scuola dell'infanzia e Istituti di istruzione). Il Comune comunica le informazioni alle ASL, alle Aziende ospedaliere, alle Regioni, nonché alle cooperative sociali ed ad altri enti che effettuano i singoli interventi di sostegno e assistenza. I dati vengono trasmessi anche all'Autorità giudiziaria per l'eventuale adozione un provvedimento di interdizione, di inabilitazione o la nomina di un amministratore di sostegno

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa all'assistenza domiciliare	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.Legge 328/2000

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti bisognosi di assistenza domiciliare e di aiuti di carattere socio-assistenziale		Stato di salute - patologie attuali Stato di salute - relativo a familiari Stato di salute - terapie in corso Stato di salute - patologie pregresse	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti bisognosi di assistenza domiciliare e di aiuti di carattere socio-assistenziale	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti bisognosi di assistenza domiciliare e di aiuti di carattere socio-assistenziale	ULSS ASL Cooperative sociali e ad altri enti (cui vengono affidate le attività di assistenza)

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori

Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna
			Lock postazione
		Virus (malware)	Firewall
			Antivirus
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT

Servizi sociali - Attività relative alla concessione di benefici economici, ivi comprese le assegnazioni di alloggi di edilizia residenziale pubblica e le esenzioni di carattere tributario

Descrizione: Con riferimento alle attività relative alla concessione di benefici, all'assegnazione degli alloggi di edilizia residenziale pubblica (che comprende anche l'attività di valutazione dei requisiti ai fini dell'eventuale riduzione dei canoni di locazione degli alloggi di proprietà comunale), nonché alle esenzioni di carattere tributario, il trattamento di dati sensibili si rende necessario sia per la concessione o l'assegnazione stesse, sia per la predisposizione delle graduatorie dei beneficiari. Le informazioni relative alla terapia in corso vengono trattate durante la fase istruttoria riguardante l'erogazione di contributi per sostenere l'acquisto di farmaci. I dati vengono forniti direttamente dagli interessati, che presentano apposita domanda al Comune, oppure da terzi (anagrafe, autorità giudiziaria, ASL, provincia, altri servizi comunali, i quali effettuano dei servizi di sostegno in favore dell'utente che versa in stato di indigenza). I dati vengono comunicati, in particolare, all'ente gestore degli alloggi che procede alla relativa assegnazione. Vengono, inoltre, effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000. Con riferimento alle attività relative alla concessione di benefici, sia in campo sociale che nel campo dello sviluppo economico, il trattamento dei dati si rende necessario sia per la concessione o l'assegnazione degli stessi, sia per la predisposizione delle graduatorie, che vengono rese pubbliche ove previsto dalla relativa normativa, fermo restando il divieto di diffondere i dati sulla salut
e

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Assegnazione di alloggi di edilizia residenziale pubblica	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. L.R. Veneto 39/2017
Concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 380/2000; Legge 241/1990, art. 12.
Attività dirette all'applicazione, anche tramite concessionari, delle disposizioni in materia di tributi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy21-9-2005 docweb 1174532. Legge 241/1990, art. 12.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti che versano in condizioni di indigenza	Dati sanitari relativi ai familiari dell'interessato	Stato di salute - patologie attuali Stato di salute - relativo a familiari Stato di salute - terapie in corso Stato di salute - patologie pregresse Dati idonei a rivelare l'origine razziale ed etnica	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti che versano in condizioni di indigenza	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Soggetti che versano in condizioni di indigenza	Trattamento dei dati personali relativi a condanne penali e reati. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy21-9-2005 docweb

controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica	1174532. Legge 241/1990, art. 12. L.R. Veneto 39/2017
Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy21-9-2005 docweb 1174532. Legge 241/1990, art. 12. L.R. Veneto 39/2017

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti che versano in condizioni di indigenza	Enti gestori di alloggi
	Amministrazioni certificanti ai sensi del DpR 445/2000

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori

Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna
			Lock postazione
		Virus (malware)	Firewall
			Antivirus
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Servizi sociali - Attività relativa alla valutazione dei requisiti necessari per la concessione di contributi, ricoveri in istituti convenzionati o soggiorno estivo (per soggetti con disabilità)

Descrizione: I dati vengono forniti dall'interessato, previa presentazione dell'istanza per accedere al contributo e/o al ricovero, ovvero da terzi (ASL o tutore, per predisporre una relazione di valutazione dello stato di non autosufficienza psico-fisica relativa all'interessato). Le informazioni sulla salute sono comunicate unicamente all'istituto che presso il quale viene effettuato il ricovero, in particolare viene comunicata l'ammissione del beneficiario, il grado di invalidità e le particolari patologie dell'interessato, al fine di garantire un'assistenza mirata. Le eventuali convinzioni religiose e filosofiche possono invece rilevare ai fini dell'erogazione di particolari regimi alimentari. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000
.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività socio-assistenziale	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 380/2000; Legge 241/1990, art. 12. Legge 104/1990

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti portatori di handicap		Dati idonei a rivelare le convinzioni religiose Stato di salute - patologie attuali Stato di salute - anamnesi familiare Dati idonei a rivelare le convinzioni filosofiche Stato di salute - terapie in corso Stato di salute - patologie pregresse Dati idonei a rivelare l'origine razziale ed etnica	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti portatori di handicap	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1 il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti portatori di handicap	istituti di ricovero Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi sociali - Attività di sostegno delle persone bisognose o non autosufficienti in materia di servizio pubblico di trasporto

Descrizione: I dati vengono forniti dall'interessato, ovvero dai suoi tutori o dai suoi curatori, i quali presentano un'apposita istanza corredata della necessaria documentazione sanitaria. Alcune informazioni possono essere acquisite anche dalla ASL in quanto i comuni, d'intesa con le aziende unità sanitarie locali, possono predisporre su richiesta dell'interessato, un progetto individuale di

integrazione e sostegno sociale. I dati vengono comunicati all'ente, all' impresa o all'associazione che effettua il servizio di trasporto. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti portatori di handicap		Stato di salute - patologie attuali	
		Stato di salute - terapie in corso	
		Stato di salute - patologie pregresse	
Soggetti che versano in condizioni di indigenza			
Soggetti in stato di non autosufficienza psico-fisica			

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti portatori di handicap	Persone giuridiche, società di persone o di capitali, imprese individuali
	Associazioni, fondazioni, enti od organismi di tipo associativo senza scopi di lucro
	Enti previdenziali e/o assistenziali

Soggetti che versano in condizioni di indigenza	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati
Soggetti in stato di non autosufficienza psico-fisica	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi sociali - Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale

Descrizione: I dati vengono forniti dall'interessato, che presenta un'apposita istanza per la fruizione dei servizi corredata della necessaria documentazione sanitaria. Questi vengono comunicati all'Ente, alle imprese ovvero alle associazioni convenzionate, alle cooperative sociali, agli organismi di volontariato ed alle ASL che provvedono all'erogazione del servizio. Per quanto concerne le attività in favore dei nomadi, idati vengono forniti direttamente dall'interessato o segnalati dalla Questura; le informazioni necessarie vengono comunicate alle associazioni del terzo settore che effettuano gli interventi.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività ricreative per la promozione del benessere della persona e della comunità, per il sostegno dei progetti di vita delle persone e delle famiglie e per la rimozione del disagio sociale	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali; Legge 328/2000; legge 104/1992
	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532; Legge 328/2000; legge 104/1992

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti in stato di disagio sociale		Dati idonei a rivelare le convinzioni religiose Stato di salute - patologie attuali Stato di salute - terapie in corso Stato di salute - patologie pregresse	

Dati idonei a rivelare l'origine
razziale ed etnica

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti in stato di disagio sociale	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti in stato di disagio sociale	Associazioni, fondazioni, enti od organismi di tipo associativo senza scopi di lucro
	ASL

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	

		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Servizi sociali - Attività relativa alle richieste di ricovero o inserimento in Istituti, Case di cura, Case di riposo, ecc

Descrizione: I dati vengono forniti da terzi (medico di base, ASL, Polizia municipale e Forze di polizia, Autorità giudiziaria) o dall'interessato, che presenta un'apposita istanza, o d'ufficio (dalle ASL e/o Aziende ospedaliere per valutare lo stato di non autosufficienza psico-fisica e per reperire le informazioni, di carattere sanitario, relative all'interessato), attraverso l'operato degli assistenti sociali: la domanda deve essere corredata della documentazione (anche sanitaria) necessaria. I dati possono essere comunicati alle ASL competenti e all'Autorità giudiziaria, al fine di avviare le procedure necessarie per il ricovero del soggetto interdetto o inabilitato presso gli istituti di cura. I dati vengono altresì comunicati ai gestori delle case di riposo ed alla direzione delle strutture residenziali, al fine di garantire l'erogazione del servizio in favore del soggetto ricoverato. Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000
.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Interventi, anche di carattere sanitario, in favore di soggetti bisognosi o non autosufficienti o incapaci	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 328/2000; legge 104/1992

il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 328/2000; legge 104/1992

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	**Categorie Particolari di Dati ex art. 9**	**Categorie relativi a condanne penali e reati ex art. 10**
Soggetti in stato di non autosufficienza psico-fisica		Dati idonei a rivelare le convinzioni religiose Stato di salute - patologie attuali Stato di salute - anamnesi familiare Dati idonei a rivelare le convinzioni filosofiche Stato di salute - terapie in corso Stato di salute - patologie pregresse Dati idonei a rivelare l'origine razziale ed etnica	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti in stato di non autosufficienza psico-fisica	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1 il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti in stato di non autosufficienza psico-fisica	ASL Altre amministrazioni ed enti pubblici Gestori delle case di riposo, alla direzione delle strutture residenziali (per l'erogazione del servizio)

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi sociali - Attività relativa ai trattamenti sanitari obbligatori (T.S.O.) ed all'assistenza sanitaria obbligatoria (A.S.O.)

Descrizione: I dati vengono acquisiti sia mediante la certificazione medica trasmessa dal servizio di igiene mentale sia tramite comunicazioni di soggetti terzi (Polizia municipale, Forze di polizia); in seguito alla redazione dell'ordinanza, viene individuato il luogo di ricovero del paziente ed inviata l'opportuna comunicazione al giudice tutelare per la convalida del provvedimento, di cui ne viene altresì data comunicazione al sindaco della città di residenza dell'interessato, che procede ad eseguire

le annotazioni di legge nel registro anagrafico ovvero al Ministero dell'interno, e al consolato competente, tramite il prefetto nel caso di cittadini stranieri o di apolidi.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Interventi, anche di carattere sanitario, in favore di soggetti bisognosi o non autosufficienti o incapaci	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 180/1978

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti con patologie psichiche		Stato di salute - patologie attuali Stato di salute - anamnesi familiare Stato di salute - terapie in corso Stato di salute - patologie pregresse	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti con patologie psichiche	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica

Soggetti con patologie psichiche	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 180/1978

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti con patologie psichiche	istituti di ricovero
	Giudice tutelare ed, eventualmente, sindaco del comune di residenza, nonché al Ministero dell'interno, e al consolato competente, tramite il prefetto nel caso di cittadini stranieri o di apolidi

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	

	Back-up eseguiti giornalmente
Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Pubblicazione atti all'Albo pretorio

Descrizione: L'attività dell'albo pretorio consiste nella pubblicazione di tutti quegli atti sui quali viene apposto il "referto di pubblicazione": deliberazioni, ordinanze, determinazioni, avvisi, manifesti, gare, concorsi e altri atti del Comune e di altri enti pubblici, che devono essere portati a conoscenza del pubblico come atti emessi dalla pubblica amministrazione; avvisi di deposito alla casa comunale di atti finanziari e delle cartelle esattoriali; provvedimenti tipo piani urbanistici, del commercio, del traffico, ecc. ecc. particolari atti riguardanti privati cittadini, come il cambio di nome e/o cognome. Nel referto di pubblicazione viene indicato l'avviso di pubblicazione e di deposito dell'atto, con l'indicazione di chi l'ha emesso o adottato, l'oggetto, la data, il numero e la precisazione dell'ufficio presso il quale il documento e gli allegati sono consultabili. La tenuta dell'albo pretorio viene curata dal personale incaricato con nomina di Messo/pubblicatore (con il Dlgs 267/2000 la figura del Messo non è piu' menzionata) che provvede a garantire la pubblicazione degli atti entro le scadenze previste, cura le affissioni e le defissioni degli Atti e vigila sulla regolare tenuta dell'albo pretorio. I documenti da pubblicare sono anche registrati nel protocollo generale.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di notifica, pubblicazione e deposito di atti, finalizzata a garantirne la conoscenza legale.	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali Legge 69/2009; DPCM 26.04.2011; D.Lgs. 33/2013

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10

Cittadini	Dati Biometrici	Dati giudiziari

Categoria particolari di dati

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali Legge 69/2009; DPCM 26.04.2011; D.Lgs. 33/2013

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori

Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna
			Lock postazione
		Virus (malware)	Firewall
			Antivirus
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

Istruzione e cultura - Gestione delle biblioteche e dei centri di documentazione

Descrizione: Alcuni dati sulle condizioni di salute possono essere acquisiti in relazione ai singoli servizi offerti all'utente (es. assistenza per il superamento di barriere architettoniche ovvero utilizzo di particolari supporti); altri dati sensibili sono trattati in relazione alle informazioni ricavabili dalle richieste relative ai singoli volumi, ai film ovvero ai documenti presi in visione o in prestito. Ulteriori dati sensibili potrebbero essere acquisiti a seguito di colloqui volti ad accertare le esigenze di studio dei richiedenti, che intendono accedere a talune sale riservate per le quali è previsto l'accesso limitato.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di promozione della cultura	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 104/1992; D.Lgs. 42/2004

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Utenti	Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche es. convinzioni alimentari)	Dati idonei a rivelare le convinzioni religiose Stato di salute - patologie attuali Dati idonei a rivelare le convinzioni filosofiche Dati idonei a rivelare le opinioni politiche	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Utenti	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Utenti	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Istruzione e cultura - Attività relativa alla gestione degli asili nido comunali e dei servizi per l'infanzia e delle scuole materne elementari e medie

Descrizione: I dati sensibili degli alunni, relativi alle specifiche situazioni patologiche del minore, possono essere comunicati direttamente dalla famiglia. Inoltre, alcune particolari scelte per il servizio di mensa (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altro genere) dei genitori degli alunni. Infine, il dato sull'origine etnica si potrebbe desumere dalla particolare nazionalità dell'interessato. Le informazioni raccolte possono essere comunicate sia ad eventuali gestori esterni del servizio mense, che provvedono all'erogazione del servizio; sia a società che effettuano il servizio di trasporto scolastico.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Gestione di asili nido e di scuole per l'infanzia	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. Legge 517/1977; legge 53/2003

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti minorenni	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Categoria particolari di dati	
		Dati idonei a rivelare l'adesione alla profilassi vaccinale obbligatoria	
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		
	Dati di contatto (numero di telefono, e-mail, ecc.)		

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti minorenni	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso
	il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale
Cittadini	

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti minorenni	Altre amministrazioni ed enti pubblici
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Autentificazione firme, foto e copie conformi

Descrizione: Il trattamento consiste nell'attestazione di conformità, apposta da un pubblico Ufficiale autorizzato, che la copia del documento esibita è uguale all'originale.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di certificazione ed autenticazione di documenti	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.P.R. 445/2000

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	

	Back-up eseguiti giornalmente
Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Personale - Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune

Descrizione: Il trattamento concerne tutti i dati relativi all'instaurazione ed alla gestione del rapporto di lavoro, avviato a qualunque titolo (compreso quelli a tempo determinato, part-time e di consulenza) nell'ente ovvero in aziende o istituzioni collegate o vigilate, a partire dai procedimenti concorsuali o da altre procedure di selezione. I dati sono oggetto di trattamento presso le competenti strutture del Comune per quanto riguarda la gestione dell'orario di servizio, le certificazioni di malattie ed altri giustificativi delle assenze; vengono inoltre effettuati trattamenti a fini statistici e di controllo di gestione. I dati sulle convinzioni religiose possono rendersi necessari per la concessione di permessi per quelle festività la cui fruizione è connessa all'appartenenza a determinate confessioni religiose; quelli sulle opinioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza o in relazione a particolari preferenze alimentari, laddove è previsto un servizio di mensa; le informazioni sulla vita sessuale possono desumersi unicamente in caso di rettificazione di attribuzione di sesso. Possono essere raccolti anche dati sulla salute relativi ai familiari del dipendente ai fini della concessione di benefici nei soli casi previsti dalla legge. I dati pervengono su iniziativa dei dipendenti e/o previa richiesta da parte del Comune. I dati vengono trattati ai fini dell'applicazione dei vari istituti contrattuali disciplinati dalla legge (gestione giuridica, economica, previdenziale, pensionistica, attività di aggiornamento e formazione). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/
2000.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica

Gestione del rapporto di lavoro	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Attività di selezione pubblica del personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Pagamento stipendi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Gestione degli adempimenti previdenziali	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Reclutamento e selezione del personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Gestione rimborsi spese	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Valutazione delle prestazioni del personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Gestione ferie e malattie	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Gestione del rapporto di lavoro del personale impiegato a vario titolo presso l'ente	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Visite mediche del personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001

Attività di controllo di gestione	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Instaurazione e gestione dei rapporti di lavoro dipendente di qualunque tipo, anche a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532.
Gestione dei contratti con i consulenti	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Programmazione del fabbisogno di personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Gestione del trattamento giuridico ed economico	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Attribuzione delle mansioni al personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Gestione delle presenze del personale	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Attività di acquisto di beni o servizi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001
Instaurazione del rapporto di lavoro	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10

Collaboratori	Curriculum Vitae	Dati idonei a rivelare l'adesione a sindacati
	Dati relativi all'esperienza professionale	Dati idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche
	Dati di contatto (numero di telefono, e-mail, ecc.)	
Soggetti partecipanti alle procedure pubbliche di selezione del personale		
Personale impiegato a vario titolo		

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Collaboratori	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1
Soggetti partecipanti alle procedure pubbliche di selezione del personale	
Personale impiegato a vario titolo	

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Collaboratori	Persone giuridiche, società di persone o di capitali, imprese individuali
Soggetti partecipanti alle procedure pubbliche di selezione del personale	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati
Personale impiegato a vario titolo	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Information asset	Cartella dipendenti	CD1		Cartella contenente i dati del personale dipendente
Information asset	Archivio personale	AP		Archivio cartaceo dei dati relativi al personale e/o collaboratori esterni dell'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Cartella dipendenti	CD1	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Sistema di gestione degli accessi alla cartella	
Archivio personale	AP	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Contenitori con chiave	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Personale / Gestione del rapporto di lavoro del personale impiegato a vario titolo presso il Comune - attività relativa al riconoscimento di benefici connessi all'invalidità

Descrizione: I dati vengono acquisiti dall'interessato e da terzi previa richiesta dell'interessato (in particolare dalla Commissione medico ospedaliera territorialmente competente per l'accertamento delle condizioni di idoneità al servizio e dal Comitato di verifica per le cause di servizio in caso di richiesta di riconoscimento di invalidità dipendente da causa di servizio e/o equo indennizzo). In caso di richiesta di pensione privilegiata, i dati vengono trasmessi all'Inpdap per l'erogazione del trattamento pensionistico. Uguale trasmissione si ha nell'ipotesi di richiesta di riconoscimento alla contribuzione figurativa di cui all'art. 80, l. n. 388/2000. Esperita l'istruttoria, la determinazione dirigenziale relativa al riconoscimento dell'invalidità viene comunicata all'INPS o alle Regioni (per gli accertamenti connessi alla liquidazione ai sensi dell'art. 130 d.lg. n. 112/1998). Vengono effettuate interconnessioni e raffronti con amministrazioni e gestori di pubblici servizi: tale tipo di operazioni sono finalizzate esclusivamente all'accertamento d'ufficio di stati, qualità e fatti ovvero al controllo sulle dichiarazioni sostitutive ai sensi dell'art. 43 del d.P.R. n. 445/2000
.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti ed abilitazioni	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Combinato disposto artt. 6.1.e. del Reg. Ue 679/2016 e parere Garante Privacy 21-9-2005 docweb 1174532. D.Lgs. 165/2001; Legge 104/1992

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Personale impiegato a vario titolo		Stato di salute - patologie attuali	
		Stato di salute - terapie in corso	
		Stato di salute - patologie pregresse	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati

Personale impiegato a vario titolo	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Personale impiegato a vario titolo	INAIL
	Inpdap

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Information asset	Cartella dipendenti	CD1		Cartella contenente i dati del personale dipendente
Information asset	Archivio personale	AP		Archivio cartaceo dei dati relativi al personale e/o collaboratori esterni dell'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	

Cartella dipendenti	CD1	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Sistema di gestione degli accessi alla cartella
Archivio personale	AP	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Contenitori con chiave
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti
			Back-up eseguiti giornalmente
		Accesso non autorizzato alla rete	Firewall
		Virus (malware)	Antivirus

SUAP

Descrizione: Gestione a mezzo portale suap delle licenze per il commercio, il pubblico esercizio, l'artigianato e le attività produttive in genere.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività relativa al rilascio di licenze, autorizzazioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	DPR 160/2010

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Imprenditori	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		Dati giudiziari

Dati di contatto (numero di telefono, e-mail, ecc.)

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Imprenditori	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	DPR 160/2010

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Imprenditori	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Servizi CAAF per ISEE

Descrizione: Attività di assistenza per la compilazione dell'ISEE

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Servizi sociali e di assistenza	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Legge 328/2000

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio) Dati relativi alla situazione reddituale (busta paga, CUD, cedolino pensione, ecc.) Dati di contatto (numero di telefono, e-mail, ecc.)	Categoria particolari di dati	

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica

Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Legge 328/2000

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Servizi demografici - Cimitero

Descrizione: Attività di assegnazione di loculi, tombe ed aggiornamento dei registri

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net
R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Assegnazione di tombe e loculi	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.Lgs. 267/2000 art. 14; D.P.R. 285/1990

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10

Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	Altre amministrazioni ed enti pubblici

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Notificazione atti e pubblicazione nell'Albo pretorio

Descrizione: Attività di notifica, pubblicazione e deposito di atti, finalizzata a garantirne la conoscenza legale a mezzo polizia municipale

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di notifica, pubblicazione e deposito di atti, finalizzata a garantirne la conoscenza legale.	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.Lgs. n. 267/2000; Legge 69/2019. CPC art. 137 e seguenti

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Categoria particolari di dati	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica

Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali D.Lgs. n. 267/2000; Legge 69/2019 D.Lgs. n. 267/2000; Legge 69/2019; Legge 890/1982; CPC art. 137 e seguenti

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo

in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	

Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Gestione deposito atti giudiziari

Descrizione: Attività di deposito di atti giudiziari, funzionale a garantirne la conoscenza legale. Servizio svolto a mezzo polizia municipale

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di notifica, pubblicazione e deposito di atti, finalizzata a garantirne la conoscenza legale.	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali Legge 69/2019; Legge 890/1982; CPC art. 137 e seguenti

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Cittadini	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Categoria particolari di dati	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Cittadini	il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Cittadini	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	Reg. UE 2016/679 Regolamento Generale per la Protezione dei Dati Personali Legge 69/2019; Legge 890/1982; CPC art. 137 e seguenti

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Cittadini	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Polizia municipale- attività di gestione delle cose ritrovate

Descrizione: Attività di gestione e conservazione delle cose ritrovate finalizzata alla riconsegna al legittimo proprietario

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Attività di gestione cose ritrovate	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	Art. 927 Codice Civile

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati

	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)		

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti a qualunque titolo interessati da rapporti con l'Ente	in relazione al presente trattamento non sono previsti destinatari ai quali vengono comunicati i dati

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	

Accesso non autorizzato alla rete	Firewall
Virus (malware)	Antivirus

Attività di inidizone e gestione di bandi e/o procedure ad evidenza pubblica

Descrizione: Il trattamento consiste nell'indizione e gestione di bandi di gara o di altre procedure di evidneza pubblica disciplinate dal codice appalti, finalizzata a selezionare sul mercato fornitori di beni e/o servizi.

Titolare del trattamento	**Nominativo**	Comune di Anguillara Veneta
	Partita IVA	01472800281
	PEC	anguillaraveneta.pd@cert.ip-veneto.net

R.P.D. / D.P.O.	**Nominativo**	Massimo Giuriati
	Partita IVA	03865868278
	E-mail	dpo@comune.anguillaraveneta.pd.it

Finalità e criteri di liceità

Finalità	Criteri di liceità ex art. 6 GDPR	Base giuridica
Gestione gare di appalto o altre procedure ad evidenza pubblica	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento	D.Lgs 50/2016

Categorie di Interessati e Categorie di dati trattati

Interessati	Dati trattati		
	Dati Comuni	Categorie Particolari di Dati ex art. 9	Categorie relativi a condanne penali e reati ex art. 10
Soggetti che versano in condizioni di indigenza	Dati sanitari relativi ai familiari dell'interessato	Stato di salute - patologie attuali Stato di salute - relativo a familiari Stato di salute - terapie in corso Stato di salute - patologie pregresse Dati idonei a rivelare l'origine razziale ed etnica	Dati giudiziari

Condizioni per il trattamento di categorie particolari di dati

Interessati	Categorie particolari di dati
Soggetti che versano in condizioni di indigenza	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1

Condizioni per il trattamento di dati personali relativi a condanne penali e reati

Interessati	Dati personali relativi a condanne penali e reati	Base giuridica
Soggetti che versano in condizioni di indigenza	Trattamento dei dati personali relativi a condanne penali e reati. Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica	D.Lgs. 50/2016
	Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.	D.Lgs. 50/2016

Categorie di destinatari ai quali i dati possono essere comunicati

Interessati	Destinatari
Soggetti che versano in condizioni di indigenza	Enti gestori di alloggi
	Amministrazioni certificanti ai sensi del DpR 445/2000

Trasferimento di dati verso paesi terzi o organizzazioni internazionali

Paesi o Organizzazioni Internazionali di destinazione	Requisiti di Trasferimento	Riferimento normativo
in relazione al presente trattamento non sono previsti trasferimenti di dati verso paesi extra UE o organizzazioni internazionali		

Asset coinvolti nel trattamento

Tipologia	Asset	Codice	Responsabili	Descrizione
Asset fisici	Personal Computer	PCA		Gruppo PC utilizzati dai soggetti autorizzati dall'Ente
Information asset	Cartella Gare & Concorsi	CGC		Cartella contenente i dati relativi alle gare di appalto e ai concorsi indetti dall'ente
Risorse IT	Server	SBB		Server Interno

Rischi e misure di sicurezza relative agli asset coinvolti nel trattamento

Asset	Codice	Rischio	Misure di Sicurezza adottate	Misure di Sicurezza ulteriori
Personal Computer	PCA	Uso dei servizi da parte di persone non autorizzate	Istruzioni sull'utilizzo delle credenziali di accesso agli strumenti elettronici e sulle loro modalità di utilizzo, fornite mediante specifico atto di nomina a soggetto autorizzato al trattamento e mediante specifica policy interna	
			Lock postazione	
		Virus (malware)	Firewall	
			Antivirus	
		Uso non autorizzato della strumentazione	Sistema di controllo degli accessi per tutti gli utenti che hanno accesso al sistema IT	
Cartella Gare & Concorsi	CGC	Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Sistema di gestione degli accessi alla cartella	
Server	SBB	Distruzione/Cancellazione dei dati	Copie di back-up conservate in supporti differenti	
			Back-up eseguiti giornalmente	
		Accesso non autorizzato alla rete	Firewall	
		Virus (malware)	Antivirus	

Conservazione dei dati

Conservazione dei dati

Interessati	Categorie di dati	Durata/Criterio di conservazione	Principali riferimenti normativi
Soggetti portatori di handicap	Dati idonei a rivelare le convinzioni religiose	10 anni	
	Stato di salute - patologie attuali	10 anni	
	Stato di salute - anamnesi familiare	10 anni	
	Dati idonei a rivelare le convinzioni filosofiche	10 anni	
	Stato di salute - terapie in corso	10 anni	
	Stato di salute - patologie pregresse	10 anni	
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni	
Soggetti che versano in condizioni di indigenza	Dati giudiziari	10 anni	

	Stato di salute - patologie attuali	10 anni
	Stato di salute - relativo a familiari	10 anni
	Dati sanitari relativi ai familiari dell'interessato	10 anni
	Stato di salute - terapie in corso	10 anni
	Stato di salute - patologie pregresse	10 anni
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni
Soggetti bisognosi di assistenza domiciliare e di aiuti di carattere socio-assistenziale	Stato di salute - patologie attuali	10 anni
	Stato di salute - relativo a familiari	10 anni
	Stato di salute - terapie in corso	10 anni
	Stato di salute - patologie pregresse	10 anni
Iscritti o candidati a partiti politici o liste civiche	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Illimitato
	Dati idonei a rivelare l'adesione a partiti	Illimitato
Soggetti in stato di non autosufficienza psico-fisica	Dati giudiziari	10 anni
	Dati idonei a rivelare le convinzioni religiose	10 anni
	Stato di salute - patologie attuali	10 anni
	Stato di salute - anamnesi familiare	10 anni
	Dati idonei a rivelare le convinzioni filosofiche	10 anni
	Stato di salute - terapie in corso	10 anni
	Stato di salute - patologie pregresse	10 anni
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni
Utenti	Dati idonei a rivelare le convinzioni religiose	10 anni
	Stato di salute - patologie attuali	10 anni
	Dati idonei a rivelare le convinzioni filosofiche	10 anni
	Dati idonei a rivelare le opinioni politiche	10 anni
	Dati idonei a rivelare convinzioni di altro genere (diverse dalle convinzioni religiose o filosofiche es. convinzioni alimentari)	10 anni
Imprenditori	Dati giudiziari	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni

	Dati di contatto (numero di telefono, e-mail, ecc.)	10 anni
Soggetti con patologie psichiche	Dati giudiziari	10 anni
	Stato di salute - patologie attuali	10 anni
	Stato di salute - anamnesi familiare	10 anni
	Stato di salute - terapie in corso	10 anni
	Stato di salute - patologie pregresse	10 anni
Commercianti	Dati giudiziari	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
Collaboratori	Dati idonei a rivelare l'adesione a sindacati	10 anni
	Curriculum Vitae	10 anni
	Dati relativi all'esperienza professionale	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
	Dati idonei a rivelare l'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	10 anni
	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni
	Dati di contatto (numero di telefono, e-mail, ecc.)	10 anni
Soggetti interessati allo svolgimento delle consultazioni elettorali	Dati giudiziari	10 anni
	Stato di salute - patologie attuali	10 anni
Soggetti a qualunque titolo interessati da rapporti con l'Ente	Dati giudiziari	10 anni
	Dati personali idonei a rivelare lo stato di salute	10 anni
	Dati relativi alla situazione reddituale	10 anni
	Dati personali idonei a rivelare la vita sessuale	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
	Dati relativi ai carichi pendenti e al casellario giudiziale	10 anni
	Dati idonei a rivelare l'origine nazionale	10 anni
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni
	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni

	Impronte digitali	10 anni
Rappresentanti e/o iscritti ad enti o associazioni senza scopo di lucro	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni
	Dati idonei a rivelare lo stato di gravidanza	10 anni
Soggetti coinvolti in violazioni in materia sanitaria o ambientale	Dati giudiziari	10 anni
	Stato di salute - patologie attuali	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
Lavoratori autonomi	Dati giudiziari	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
Soggetti minorenni	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
	Dati idonei a rivelare il rapporto di parentela	10 anni
	Dati idonei a rivelare lo stato di disabilità	10 anni
	Categoria particolari di dati	10 anni
	Dati idonei a rivelare l'adesione alla profilassi vaccinale obbligatoria	10 anni
	Dati idonei a rivelare caratteristiche o idoneità psico-fisiche	10 anni
Cittadini	Dati giudiziari	Illimitatamente
	Dati personali idonei a rivelare lo stato di salute	Illimitatamente
	Dati idonei a rivelare le convinzioni religiose	Illimitatamente
	Stato di salute - patologie attuali	Illimitatamente
	Dati personali idonei a rivelare la vita sessuale	Illimitatamente
	Dati Biometrici	Illimitatamente
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Illimitatamente
	Stato di salute - relativo a familiari	Illimitatamente
	Dati relativi ai carichi pendenti e al casellario giudiziale	Illimitatamente
	Dati relativi ad altri provvedimenti o procedimenti giudiziari	Illimitatamente

	Categoria particolari di dati	Illimitatamente
	Stato di salute - terapie in corso	Illimitatamente
	Stato di salute - patologie pregresse	Illimitatamente
	Dati idonei a rivelare l'origine razziale ed etnica	Illimitatamente
	Dati relativi alla situazione reddituale (busta paga, CUD, cedolino pensione, ecc.)	Illimitatamente
	Dati di contatto (numero di telefono, e-mail, ecc.)	Illimitatamente
Soggetti in stato di disagio sociale	Dati idonei a rivelare le convinzioni religiose	10 anni
	Stato di salute - patologie attuali	10 anni
	Stato di salute - terapie in corso	10 anni
	Stato di salute - patologie pregresse	10 anni
	Dati idonei a rivelare l'origine razziale ed etnica	10 anni
Personale impiegato a vario titolo	Stato di salute - patologie attuali	10 anni
	Stato di salute - terapie in corso	10 anni
	Stato di salute - patologie pregresse	10 anni
Soggetti coinvolti in incidenti e/o infortuni stradali	Stato di salute - patologie attuali	10 anni
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	10 anni
	Stato di salute - terapie in corso	10 anni
Soggetti richiedenti licenze o autorizzazioni amministrative	Dati giudiziari	Illimitatamente
	Dati anagrafici (nome, cognome, sesso, luogo e data di nascita, residenza, domicilio)	Illimitatamente

COMUNE di
ANGUILLARA VENETA
www.comune.anguillaraveneta.pd.it

ALLEGATO "C" DELIBERA DI GIUNTA N. 91 DEL 31/10/2019

Regolamento per l'utilizzo dei sistemi e strumenti informatici di Comune di Anguillara Veneta

COMUNE di
ANGUILLARA VENETA
www.comune.anguillaraveneta.pd.it

Indice

COMUNE di
ANGUILLARA VENETA
www.comune.anguillaraveneta.pd.it

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone l'ente a responsabilità di natura civile, penale e amministrativa.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, **l'ente** ha adottato un Regolamento interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti i dipendenti a mezzo delle nomine a soggetti autorizzati al trattamento ex art. 29 del Reg. UE 2016/679, nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del Reg. UE 2016/679, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse, come previsto dall'art. 4-3°comma dello Statuto dei lavoratori.

Il presente regolamento inoltre costituisce, insieme alle altre procedure interne adottate e al registro dei trattamenti, uno degli elementi che compone il sistema di gestione di protezione dei dati personali dell'ente.

1. Entrata in vigore del Regolamento e pubblicità

1.1 Il nuovo Regolamento entrerà in vigore con l'avvenuta esecutività della deliberazione di Giunta Comunale che lo approva. Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

1.2 Copia del Regolamento, oltre ad essere affisso nella bacheca dell'ente, verrà consegnato a ciascun dipendente, anche ai fini dell'art. 13 Reg. UE 2016/679 e dell'art.4, comma 3°, dello Statuto dei lavoratori. Il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare dell'ente.

2. Campo di applicazione del Regolamento

2.1 Il nuovo Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori e consulenti a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori coordinati e continuativi, in stage, etc.) che venissero autorizzati a far uso di strumenti tecnologici dell'ente o perfino di accedere alla rete informatica aziendale e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, le regole di seguito previste devono intendersi a carico tanto dei primi quanto dei secondi, ferma restando la necessità che si dia opportuno conto del presente Regolamento nel contratto concluso con quest'ultimi.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "soggetto autorizzato al trattamento", ai fini del Reg. UE 2016/679, in ragione delle attività e degli impegni che si assume nell'organizzazione aziendale od a favore dell'ente stesso.

3. Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete del Comune di Anguillara Veneta solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 L'ente rende noto che il soggetto responsabile del servizio Information and Communication Tecnology (nel seguito per brevità "Servizio ICT") Ditta Servizi Informatici di El Djazairli Davide è stato autorizzato dall'ente a compiere interventi nel sistema informatico diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio ITC ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

3.4 Il servizio ICT ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 **Non è consentito** l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'ente a gravi responsabilità civili e amministrative; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente.

3.6 Salvo preventiva espressa autorizzazione, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

3.7 Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In caso di assenza temporanea, l'utilizzatore è tenuto a bloccare la postazione attraverso la sequenza CTRL + ALT + CANC.

4. Gestione e assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate previa formale richiesta del Responsabile dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id) associato ad una parola chiave (password) riservata che dovrà venir **custodita dall'incaricato con la**

massima diligenza e non divulgata.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili al soggetto autorizzato.

4.4 Qualora la parola chiave dovesse venir sostituita, per decorso del termine di vita e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio ICT.

5. Utilizzo della rete

5.1 Per l'accesso alla rete ciascun utente deve utilizzare la propria credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del Servizio ICT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato del Servizio ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.4 Il personale del Servizio ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC dei soggetti autorizzati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5.6 Nella gestione dei sistemi informatici, il servizio ICT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto 12.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3.3., e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

6. Utilizzo di altri dispositivi elettronici

6.1 **Tutti i dispositivi elettronici dati in dotazione al personale dell'ente devono considerarsi strumenti di lavoro:** ne viene concesso l'uso esclusivamente per lo svolgimento delle attività lavorative, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività lavorative. Fra i dispositivi in questione vanno annoverati i telefoni aziendali, PC

portatili, tablet, telefoni cellulari, smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete o di condividere documenti, dati e materiali ivi conservati e/o trattati.

6.2 L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni.

6.3 Con riferimento ai telefoni aziendali e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite da parte dell'ente.

6.4 Si precisa, peraltro, che le disposizioni previste nel presente Regolamento ai punti 3, 7, 8, 9, 10 e 11 dello stesso trovano applicazione anche nell'uso dei dispositivi elettronici qui considerati.

6.5 Viene infine disposto il divieto di utilizzo per fini personali di fax aziendali, per spedire o per ricevere documentazione, e/o di fotocopiatrici aziendali, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

7. Utilizzo e conservazione dei supporti rimovibili

7.1 In caso di utilizzo di supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili, questi devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

7.3 Viene severamente vietato l'utilizzo di supporti rimovibili personali.

7.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio ICT e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del Servizio ICT.

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica ***nomecognome@ente.it*** per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale del Servizio ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza commerciale e soprattutto allegati ingombranti. In caso di cessazione del rapporto di lavoro, il singolo dipendente è tenuto ad eliminare dalle proprie cartelle tutti i messaggi di posta elettronica ed i documenti non pertinenti l'attività dell'ente e non utili alle esigenze lavorative, mantenendo integra, invece, tutta la corrispondenza e documentazione inerente alla attività lavorativa. Resta inteso che, di conseguenza, la documentazione presente nel profilo del singolo utente che cessa il rapporto di lavoro verrà considerata presuntivamente dall'ente quale corrispondenza e documentazione lavorativa e non personale.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'ente ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

8.5 Poiché la casella di posta assegnata costituisce strumento di lavoro, è opportuno evidenziare che i messaggi ivi contenuti, avendo presuntivamente natura di corrispondenza commerciale, verranno conservati nei server ente per 10 anni, a norma dell'art. 2220 del Codice civile

8.6 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

8.7 È obbligatorio porre la massima attenzione nell'aprire gli allegati di posta elettronica se non si è certi della loro provenienza. Usare prudenza anche se un messaggio provenienza da un indirizzo conosciuto. In caso di dubbio l'utente dovrà rivolgersi al personale del Servizio ICT.

8.8 Al fine di garantire la funzionalità del servizio di posta elettronica e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata e disattivata dall'utente.

8.9 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura del responsabile dell'ufficio.

8.10 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'ente, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 8.7; assenza non programmata ed impossibilità di attendere i due giorni di cui al punto 8.8).

8.11 Il personale del Servizio ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 3.3.

8.12 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente autorizzato dall'ente potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy.

8.13 L'ente si riserva la facoltà, a proprio insindacabile giudizio, di assegnare o ritirare l'utilizzo della casella di posta elettronica in base alla propria esclusiva e insindacabile valutazione della necessità di utilizzo della stessa per lo svolgimento delle attività lavorative.

8.14 La casella di posta elettronica, unitamente alle credenziali di autenticazione per l'accesso alla rete, viene disattivata al momento della conclusione del rapporto di lavoro che ne giustificava l'assegnazione. L'ente si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità aziendale; in tal caso:
- avranno accesso alla casella esclusivamente dipendenti individuati dall'ente in funzione alle mansioni lavorative assegnate;
- verranno inviate mail ai mittenti con indicazione della diversa casella di posta elettronica dell'ente cui trasmettete i messaggi;
- viene escluso, comunque, l'invio di messaggi da tale casella di posta.

8.15 Nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata, tale utente dovrà attenersi alle regole previste nell'ulteriore apposito Regolamento a ciò dedicato e che va comunque a completare ed integrare il presente Regolamento.

9. Navigazione in Internet

9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:
- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'iscrizione con account aziendale e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'ente rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una "black list".

9.4 Gli eventuali controlli, compiuti dal personale incaricato del Servizio ICT ai sensi del precedente punto 3.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 24 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'ente.

9.5 L'utilizzo di tutte le reti WiFi presenti è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal reparto ICT.

9.6 L'accesso da remoto alla rete è possibile agli utenti abilitati solo a seguito di comunicazione di specifiche credenziali o dell'installazione di software che lo abilita sui dispositivi in uso.

9.7 L'accesso da remoto alla rete è possibile solo utilizzando i dispositivi previsti. A tale scopo vengono svolti controlli automatici che impediscono l'accesso utilizzando dispositivi non abilitati.

10. Protezione antivirus

10.1 Il sistema informatico dell'ente è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio ICT.

10.3 Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio ICT.

11. Partecipazioni a social media

11.1 L'utilizzo a fini promozionali e commerciali dei social media – quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dall'ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti (conformemente a quanto disposto al precedente punto 9.2).

11.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, l'ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'ente, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dall'ente, sia che utilizzino propri dispositivi, sia che

partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti dell'ente.

11.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui fornitori ed altri partners. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'ente. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione da parte dell'ente.

11.4 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio.

11.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi o colleghi, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito lavorativo.

11.6 Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Responsabile d'ufficio, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'ente.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di protezione dei dai dati personali, come indicato nella lettera di designazione a soggetto autorizzato al trattamento ex art. 29 Reg. UE 2016/679.

12.2 Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 13, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico dell'ente ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti (conformemente al successivo punto 14), fermo restando il rispetto della normativa in materia di protezione dei dati personali (Reg. UE 2016/679).

12.3 Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio, l'ente provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'ente, tramite il personale del Servizio ICT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure di cui ai precedenti 3.3. e 3.4, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Sistemi di controlli graduali

14.1 In caso di anomalie, il personale incaricato effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie.

14.2 In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

15. Sanzioni

15.1 È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL applicato, e nei confronti dei soggetti di cui all'1.2, verificata la gravità della violazione contestata, con la risoluzione od il recesso dal contratto ad essi relativo nonché con tutte le azioni civili e penali consentite.

16. Aggiornamento e revisione

16.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate da parte dell'ente.

16.2 Il presente Regolamento è soggetto periodicamente a revisione.

DATA BREACH E PROCEDURA PER LA GESTIONE DEGLI EVENTI

I Premessa

Con il termine data breach, ai sensi degli artt. 33 e 34 del Reg. UE 679/2016, s'intende la violazione dei dati personali dell'interessato persona fisica, che può consistere, a titolo esemplificativo e non esaustivo (Considerando 85 del Regolamento), in:

- perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti;

- discriminazione, furto o usurpazione d'identità;

- perdite finanziarie, decifratura non autorizzata della pseudonimizzazione;

- pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale;

- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

II Le tipologie di violazione dei dati personali

In linea con la definizione di violazione di dati personali, ex art. 4 p.12 Reg. UE, possiamo distinguere 3 tipi di violazione, che possono tuttavia combinarsi tra loro:

1) violazione di riservatezza, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.

2) Violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale.

3) Violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

III Cosa prescrive a riguardo il Regolamento UE?

A. Art. 33: Notifica al Garante.

Il Regolamento UE prescrive che il ***titolare***, non appena viene a conoscenza di un'avvenuta violazione dei dati personali del trattamento, dovrebbe notificare la violazione al Garante della Privacy, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza del Data breach. Se non effettuata entro 72 ore, deve essere fornita una giustificazione per il ritardo.

Che cosa deve contenere la notifica?

A norma dell'art. 33 *la notifica deve almeno:*

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili conseguenze della violazione dei dati personali;

d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Resta fermo che *qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*

Al fine di semplificare la procedura, l'autorità Garante ha predisposto un Pdf editabile da compilare, firmare digitalmente ed inviare per ottemperare all'obbligo di notifica, scaricabile al seguente url: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835.

La notifica è sempre un obbligo in caso di data breach?

No. La notifica non è dovuta se risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Tale evenienza si verifica, per esempio, allorché siano state efficacemente attuate misure tecnologiche di cifratura o pseudonimizzazione che rendano improbabile ricostruire l'origine del dato, oppure quando il dato è inidoneo a rivelare alcunché di pregiudizievole o comunque riservato circa l'interessato.

B. Art. 34: Comunicazione all'interessato.

In aggiunta all'obbligo di notifica all'autorità di controllo, è previsto l'obbligo di comunicare, in un linguaggio semplice e chiaro, la violazione dei dati personali allo stesso interessato allorché tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Cosa deve contenere la comunicazione?

A norma dell'art. 34 la comunicazione, la cui forma è libera, deve obbligatoriamente:

- rappresentare *il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;*

- *descrivere le probabili conseguenze della violazione dei dati personali;*

- *descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.*

La comunicazione, ove la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è sempre un obbligo in caso di data breach?

No. Anche ove sussistessero tali condizioni, l'art. 34 esonera il titolare dall'obbligo di comunicazione allorché sia soddisfatta almeno una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

IV Data breach e regimi particolari

Il Garante della Privacy nazionale ha mantenuto i provvedimenti a specificazione ulteriore delle norme del Regolamento, sicché sussistono 4 ipotesi di Data breach in deroga alle disposizioni generali sopra richiamate, che richiedono una tempistica più stringente di attivazione da parte del titolare, ovvero:

Tipologia	*Riferimento normativo*	*Timing imposto*	*Url doc web*
SOCIETA' TELEFONICHE E INTERNET PROVIDER	Provvedimento del Garante n. 161 del 4 aprile 2013	24 ore notifica; 72 ore comunicazione → (in entrambi i casi dalla scoperta dell'evento)	doc. web n. 2388260 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2388260
TRATTAMENTO DATI BIOMETRICI	Provvedimento n. 513 del 12 novembre 2014	Entro 24 ore dalla conoscenza del fatto	doc. web n. 3556992 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992
DOSSIER SANITARIO ELETTRONICO	Provvedimento n. 331 del 4 giugno 2015	Entro 48 ore dalla conoscenza del fatto	doc. web n. 4084632 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4084632
AMMINISTRAZIONI PUBBLICHE	Provvedimento n. 392 del 2 luglio 2015	Entro 48 ore dalla conoscenza del fatto	doc. web n. 4129029 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4129029

Come da infografica del Garante riportata in calce, ove si ricada in una delle tipologie, dovrà anche aversi cura di utilizzare lo specifico modello di volta in volta individuato dal Garante per notificare la violazione riscontrata.

Violazioni di dati personali *(data breach)*

Gli adempimenti previsti

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante per la protezione dei dati personali ha adottato una serie di provvedimenti che fissano per amministrazioni pubbliche e aziende l'obbligo di comunicazione nei casi in cui - a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità - si dovesse verificare la perdita, la distruzione o la diffusione indebita di dati personali conservati, trasmessi o comunque trattati. La scheda, che ha mere finalità divulgative, riassume i casi finora esaminati.

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Art. 32-*bis* del Codice in materia di protezione dei dati personali (d. lgs. 196/2003), Regolamento UE 611/13, Provvedimento del Garante n. 161 del 4 aprile 2013 [doc. web n. 2388260]

- **L'obbligo di comunicazione al Garante** *(mediante un apposito modello di comunicazione)* riguarda i fornitori di servizi telefonici e di accesso a Internet (e non, ad esempio, i siti internet che diffondono contenuti, i motori di ricerca, gli *internet point*, le reti aziendali).
- In caso di violazione dei dati personali, società di tlc e Isp **devono**:
  a. **entro 24 ore** dalla scoperta dell'evento, fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione
  b. **entro 3 giorni dalla scoperta,** informare anche ciascun utente coinvolto, comunicando gli elementi previsti dal Regolamento 611/2013 e dal provvedimento del Garante n. 161 del 4 aprile 2013.
- La comunicazione agli utenti **non è dovuta** se si dimostra di aver utilizzato misure di sicurezza nonché sistemi di cifratura e di anonimizzazione che rendono inintelligibili i dati. Nei casi più gravi, il Garante può comunque imporre la comunicazione agli interessati.
- Per consentire l'attività di accertamento del Garante, società telefoniche e provider devono tenere un **inventario** costantemente aggiornato delle violazioni subite.
- **SANZIONI AMMINISTRATIVE PREVISTE (art. 162-*ter* del Codice in materia di protezione dei dati personali)**
  - per mancata o ritardata comunicazione al Garante: da 25mila a 150mila euro;
  - per omessa o mancata comunicazione agli utenti: da 150 euro a 1000 euro per ogni società, ente o persona interessata;
  - per mancata tenuta dell'inventario delle violazioni aggiornato: da 20mila a 120mila euro.

BIOMETRIA

Provvedimento n. 513 del 12 novembre 2014 [doc. web n. 3556992]

- **Entro 24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) comunicano al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

- **Entro 48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

AMMINISTRAZIONI PUBBLICHE

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

- **Entro 48 ore** dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante *(tramite il modello allegato al provvedimento)* tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

Per approfondimenti, consultare i provvedimenti pubblicati sul sito: www.garanteprivacy.it

V Obblighi generali in capo al titolare del trattamento dei dati

Oltre alle specifiche richiamate dal Regolamento in ordine alle tecnologie che devono essere adottate per trattare i dati personali in sicurezza, l'art. 32 all'ultimo comma dispone che *il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali* (ovvero gli incaricati) *non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*.

E' dunque quantomai opportuno che il titolare predisponga lettere di incarico precise ai responsabili ed agli incaricati, e fornisca loro adeguata formazione circa gli obblighi derivanti da *Data breach.*

Parimenti (art. 32.5) è fatto obbligo per **il titolare** ***di documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio***. *Tale documentazione consente all'autorità di controllo di verificare il rispetto* delle disposizioni di legge (cd. inventario delle violazioni).

Si ricorda che l'obbligo di notifica spetta al titolare, che pertanto è chiamato a verificare preventivamente l'idoneità del responsabile del trattamento, specie se trattasi di un fornitore di servizi esterno all'azienda, a gestire tempestivamente ed adeguatamente un data breach, anche prevedendo, a norma dell'art. 28 del Regolamento, idonei accordi che regolino il rapporto di fornitura in modo da garantire il rispetto del Regolamento.

L'uso dei servizi *Cloud* di archiviazione dati, infine, richiede una particolare attenzione da parte del titolare del trattamento, giacché il *Cloud* generalmente spoglia il titolare del trattamento della possibilità di ingerirsi nella gestione del sistema informatico. In tal caso il titolare del trattamento, oltre a verificare preventivamente che il servizio in *Cloud* abbia specifiche conformi al Regolamento Ue, *in primis* circa l'ubicazione dei server e le condizioni generali di contratto, dovrà anche monitorare sistematicamente il registro dei log e degli eventi, per verificare eventuali violazioni dei dati personali, specie in punto accessi non autorizzati di terzi.

VI Criteri per determinare l'opportunità della notifica

La qualificazione della violazione del Data breach è rimessa sostanzialmente al titolare, sulla base della valutazione tanto della qualità del dato, quanto dei sistemi tecnologici a presidio dello stesso. Ed invero, a fronte della perdita di dati estremamente sensibili, un efficace sistema di anonimizzazione potrebbe rendere superfluo procedere alla notifica. Nel dubbio, tuttavia, è opportuno adottare la soluzione maggiormente in linea con le esigenze di tutela richiamate dal Regolamento.

In via preliminare si rimanda alle **linee guida WP 29 aggiornate al 6 febbraio 201**8, che forniscono una casistica di situazioni tipo che un titolare del trattamento può essere chiamato ad affrontare in presenza di una Data Breach. Ove il caso concreto sfugga alla casistica elencata, criteri per potere compiere tale scelta consapevolmente sono stati individuati dall'European Union Agency for Network and Information Security (ENISA), nel documento chiamato "Recommendations for a methodology of the assessment of severity of personal data breaches".

WORKFLOW PROCEDURA DATA BREACH

VII Procedura per la gestione degli eventi in azienda

1. L'incaricato al trattamento ravvisa un incidente nella gestione dei dati che astrattamente può determinare un data breach ai sensi del regolamento.
2. Viene senza indugio informato il titolare/responsabile, che di concerto con l'amministratore di sistema, nel caso il data breach si riferisca al trattamento dati effettuato con strumenti informatici, procedono alla valutazione d'impatto dell'incidente in relazione ai diritti degli interessati, utilizzando nell'ordine: la casistica offerta dal WP 29, la procedura ENISA.

   Nel caso l'incidente sia ravvisato direttamente dall'amministratore di sistema, egli deve senza indugio notiziare il titolare e procedere di concerto alla valutazione d'impatto.

   Se nominato, il DPO deve essere informato e messo nelle condizioni di partecipare.
3. In base all'esito della verifica:
   a) se il data breach non risulta presentare alcun rischio per gli interessati, non si provvede ad alcuna notifica né all'autorità di controllo né agli interessati. Si procede comunque ad annotare nell'apposito registro l'incidente. Nel caso di responsabile esterno, il report deve essere trasmesso anche al titolare. Parimenti nel caso di contitolarità del trattamento, tutti devono essere notiziati dell'evento.
   b) Se il data breach risulta presentare rischi per gli interessati, si procede conformemente allo schema del WP 29 allegato, oppure in base alla procedura ENISA, così da stimare la gravità del rischio per procedere alla notifica alla sola autorità garante (o all'autorità capofila nel caso l'incidente coinvolga interessati di diversi stati membri), financo ai singoli individui, utilizzando il modulo allegato.
4. In ogni caso tutti gli incidenti devono confluire in un registro conservato a cura del titolare a mezzo di ristretti incaricati conformemente alla lettera di nomina.

Costituiscono allegati al presente modulo, e parte integrante dello stesso:

1) Linee guida WP 29 Data Breach;
2) Casistica WP 29 in Italiano (fonte: Italia Oggi, 14 marzo 2018 serie speciale nr.5);
3) Procedura ENISA valutazione di impatto degli incidenti;
4) Excel con formule per applicazione della procedura ENISA;
5) Registro delle violazioni in formato Excel;
6) Modello di comunicazione agli interessati.

Casistica WP 29 in Italiano (fonte: Italia Oggi, 14 marzo 2018 serie speciale nr.5)

Casi	Notificare all'Autorità sdi Controllo	Comunicazione agli Interessati	Note
1. Un Titolare del Trattamento ha conservato copia di un archivio di dati personali criptati su un CD. Il CD viene rubato	No	No	Fino a che i dati vengono crittografati con un algoritmo avanzato, esistono backup dei dati e la chiave univoca non è compromessa, questa non è una violazione da segnalare. Tuttavia, se i dati vengono successivamente compromessi, è necessaria la notifica
2. Dati personali vengono esportati da un sito internet sicuro gestito dal titolare del trattamento durante un attacco informatico. Il titolare del trattamento ha clienti in un singolo Stato della Ue	Si, bisogna notificare l'Autorità di Controllo se ci sono potenziali conseguenze per i singoli interessati	Si, dipende dalla natura dei dati personali affetti e dalla gravità delle conseguenze per i singoli interessati	

Casi	Notificare all'Autorità sdi Controllo	Comunicazione agli Interessati	Note
3. Un breve black-out, della durata di alcuni minuti, impedisce il funzionamento dei call center del titolare del trattamento. Di conseguenza i clienti non possono accedere ai loro dati	No	No	Non si tratta di una violazione dei dat personali da segnalare, ma si tratta comunque di un incidente registrabile ai sensi dell'articolo 33(5). Appropriata registrazione devono essere conservati dal titolare del trattamento
4. Il titolare del trattamento subisce un attacco ransomware che provoca la crittografia di tutti i dati. Non sono disponibili back-up e i dati non possono essere ripristinati. Durante le indagini, diventa chiaro che l'unica funzionalità del ransomware era quella di crittografare i dati e che non vi erano altri malware presenti nel sistema	Sì, riferire all'autorità di vigilanza competente, se ci sono potenziali conseguenze per gli individui in quanto si tratta di una perdita di disponibilità di dati.	Sì, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze	Se fosse disponibile una copia di riserva e i dati potessero essere ripristinati in tempo utile, ciò non dovrebbe essere segnalato all'autorità di vigilanza o agli Interessati in quanto non vi sarebbe stata alcuna perdita permanente di disponibilità o riservatezza dei dati. Tuttavia, l'autorità di controllo può prendere in considerazione un'inchiesta per valutare la conformità ai requisiti di sicurezza dell'articolo 32
5. Un cliente telefona al call center di una banca per segnalare una violazione dei dati poiché ha ricevuto una dichiarazione mensile del conto bancario non proprio	Sì	Solo le persone interessate vengono avvisate se c'è un rischio elevato ed è chiaro che altri non sono stati colpiti	Se, dopo ulteriori indagini, viene identificato un numero maggiore di persone interessate, è necessario eseguire un aggiornamento dell'autorità di vigilanza e il controllore effettua il passaggio aggiuntivo per notificare agli altri individui se vi è un rischio elevato per loro

Il titolare del trattamento intraprende una breve indagine (completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se si tratta di un difetto sistemico che ha o potrebbe interessare altri clienti			
6. Un mercato online multinazionale subisce un attacco informatico e nomi utente, password e cronologia degli acquisti sono pubblicati online dall'autore dell'illecito	Sì, segnalare all'autorità di vigilanza capofila se comporta l'elaborazione transfrontaliera	Sì, già che ci possono essere conseguenti rischi	Il titolare del trattamento dovrebbe agire, ad es. forzando il ripristino della password degli account interessati, nonché altri passaggi per mitigare il rischio
7. Una società di hosting di siti web (responsabile del trattamento) identifica un errore nel codice che controlla l'autorizzazione dell'utente. Ciò implica che ogni utente possa accedere ai dettagli dell'account di qualsiasi altro utente	Come responsabile del trattamento, la società di hosting di siti Web deve informare i suoi clienti interessati (i titolari del trattamento) prontamente. Supponendo che la società di hosting abbia condotto la propria indagine, i titolari del trattamento interessati dovrebbero essere ragionevolmente fiduciosi sul fatto che tutti abbia subito una violazione e quindi è vengono considerati come "informati" una volta che sono stati notificati dalla società di hosting (responsabile del trattamento)	Se non ci sono alti rischi per i singoli interessati, essi non devono essere avvisati	La società di hosting del sito web (titolare del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS). Se non vi è alcuna prova che questa vulnerabilità sia sfruttata con questo particolare responsabile del trattamento, una violazione notificabile potrebbe non essersi verificata ma potrebbe essere registrabile o essere oggetto di non conformità ai sensi dell'articolo 32

Casi	Notificare all'Autorità sdi Controllo	Comunicazione agli Interessati	Note
	I titolari del trattamento devono quindi informare l'autorità di vigilanza		
8. Le cartelle cliniche di un ospedale non sono disponibili per un periodo di 30 ore a causa di un attacco informatico	Sì, l'ospedale è obbligato a notificare già che ci possono essere gravi conseguenze per il benessere del paziente e la sua privacy	Sì, comunicare alle persone colpite	
9. I dati personali di 5000 studenti vengono erroneamente inviati alla mailing list sbagliata con oltre 1000 destinatari	Sì, riferire all'autorità di vigilanza	Sì, comunicare gli interessati in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	
10. Una e-mail di marketing diretto viene inviata ai destinatari nel campo "a:" o "cc:", consentendo in tal modo a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari	Sì, la notifica all'autorità di vigilanza può essere obbligatoria se un numero elevato di persone è interessato, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la posta contiene password)	Sì, comunicare agli interessati in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato solo un numero minore di indirizzi e-mail

DATA BREACHES. COMUNICAZIONI AGLI INTERESSATI

(ex raccomandazione WP 29-2018)

I data breaches devono essere comunicati agli interessati direttamente dalla violazione (a mezzo mail preferibilmente, o sms), salvo ciò non comporti sforzi sproporzionati in ragione dell'ampia platea degli stessi. In tale caso è ammesso, a norma dell'art. 34, una comunicazione pubblica (a mezzo sito web) o altre misure efficaci equivalenti.

E' essenziale che si utilizzi una lingua effettivamente conosciuta dall'interessato.

Spett.le___

Indirizzo di contatto _____-

In qualità di interessato ci duole informarLa che in data _____ è stata riscontra una violazione dei suoi dati personali.

Descrizione della natura dell'incidente e dei dati personali interessati:

Xxxx

Descrizione delle probabili conseguenze della violazione:

Xxxx

Descrizione delle misure già adottate e che saranno adottate per minimizzare gli effetti delle violazione:

Xxxx

Suggerimenti per minimizzare gli effetti della violazione:

Xxxx

Informazioni di contatto del titolare o del DPO:

Xxxx