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.

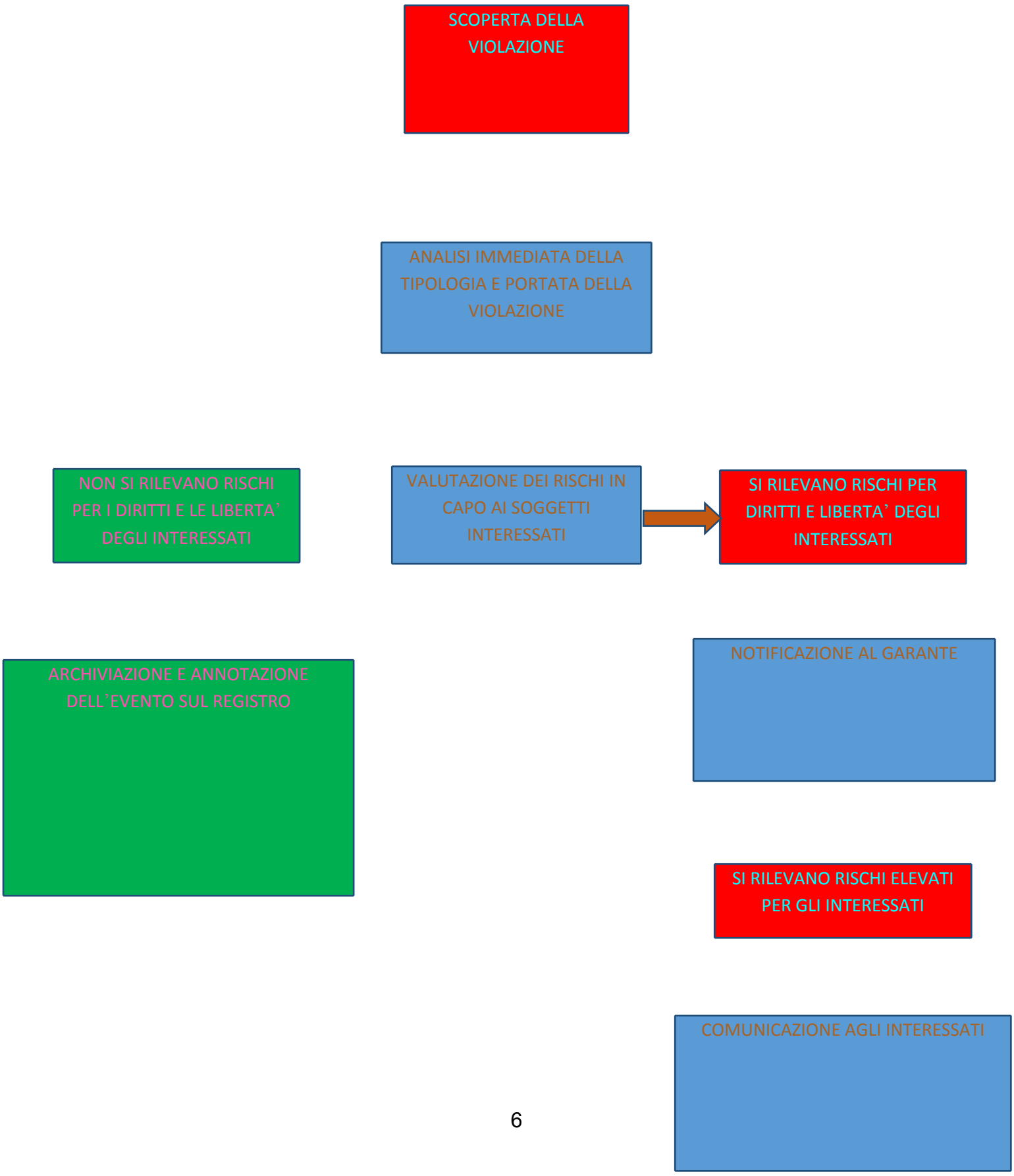
L'uso dei servizi *Cloud* di archiviazione dati, infine, richiede una particolare attenzione da parte del titolare del trattamento, giacché il *Cloud* generalmente spoglia il titolare del trattamento della possibilità di ingerirsi nella gestione del sistema informatico. In tal caso il titolare del trattamento, 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.