CIRCOLARE N. 2-2018

IL DATA BREACH: PROFILI OPERATIVI

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

1. SCENARIO NORMATIVO

Dal 25 maggio 2018, in virtù del disposto degli articoli 33 e 34 del RGPD (Regolamento UE 2016/679), diventeranno operative le nuove prescrizioni in materia di violazione della sicurezza, da cui derivi una violazione dei dati personali (c.d. "data breach").

Di regola, tutti i titolari di trattamento (TdT), dovranno notificare un data breach all'Autorità di controllo e comunicare l'accaduto a tutti gli interessati.

L'obbligo non è assoluto, ricorrendo alcune eccezioni, collegate alla preventiva neutralizzazione di fattori di rischio per le persone fisiche interessate.

Le norme sono stringenti quanto a soggetti legittimati passivi e modalità di effettuazione delle dovute notificazioni e comunicazioni.

Quanto ai soggetti tenuti si registra una estensione a tutti i titolari di trattamento, senza esclusioni aprioristiche o inclusioni riservate a specifiche per categorie (di trattamento o di dati personali).

È previsto, poi, che le notificazioni all'Autorità di Controllo siano perfezionate entro 72 ore e comunque "senza ingiustificato ritardo" dal momento in cui si è avuta consapevolezza dell'accaduto.

La notificazione all'Autorità di controllo deve descrivere la natura della violazione dei dati personali compresi le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; deve, inoltre, descrivere le probabili conseguenze della violazione dei dati personali; deve, infine, 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.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo". Fanno eccezione alcune ipotesi.

Non è richiesta la comunicazione all'interessato quando è presente 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) la 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.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

Il Gruppo "Articolo 29" (WP29) ha diramato proprie linee-guida in materia di notifica delle violazioni di dati personali (WP250rev.01, Guidelines on Personal data breach notification under Regulation 2016/679, Adopted on 3 October 2017, As last Revised and Adopted on 6 February 2018). Allo scopo di fornire un vademecum pratico per la gestione dell'adempimento si esaminano alcuni punti nodali della disciplina.

2. NOZIONE DI DATA BREACH

Le linee guida cristallizzano il seguente principio: "mentre tutti le violazioni dei dati sono violazioni di sicurezza, non tutte le violazioni di sicurezza sono necessariamente violazione dei dati".

Ai fini delle incombenze previste dalla disciplina del "data breach" rilevano le violazioni di sicurezza da che esitano in violazione dei dati, articolate nei seguenti tipi:

a) violazioni della riservatezza, e cioè disvelamento o accesso indebito o accidentale ai dati;

b) violazioni della disponibilità dei dati, e cioè indebito o accidentale impedimento all'accesso di dati o distruzione di dati;

c) violazione della integrità dei dati, e cioè indebita o accidentale alterazione dei dati.

Con riferimento ai dati, il WP29 censisce le seguenti evenienze:

- distruzione, ovvero attività da cui deriva la perdita definitiva di dati o la perdita definitiva della possibilità di utilizzo per il Titolare Del Trattamento;
- danneggiamento, ovvero alterazione, corruzione, riduzione della integrità
- perdita di dati, ovvero inibizione all'accesso, perdita di controllo e perdita di accesso a dati, che continuano a sussistere

3. TERMINI

L'obbligo di notificazione all'autorità di controllo deve essere adempiuto entro 72 ore.

In pratica si pone il quesito della decorrenza del termine, in particolare nei casi in cui il trattamento sia effettuato da un responsabile del trattamento (RdT) nel caso di esternalizzazione dei trattamenti stessi.

La risposta fornita dalle Linee Guida del WP29 (con un mutamento di opinione sostanziale rispetto a una versione originaria del documento) si attesta a considerare rilevante il momento in cui diventa consapevole della violazione il titolare del trattamento:

> *"in principle, the controller should be considered as "aware" once the processor has informed it of the breach".*

Non si tratta, si badi bene, di una postdatazione arbitraria del termine iniziale, in quanto da un punto di vista giuridico formale il trattamento svolto dal responsabile del trattamento per conto del titolare del trattamento è, in ogni caso e ad ogni effetto, imputabile a quest'ultimo.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

Pertanto si invita a non considerare il principio sopra riportato quale atto a giustificare eventuali dilazioni nel passaggio delle notizie dal responsabile al titolare del trattamento.

Tutto ciò pone, naturalmente, un problema nei rapporti tra titolare e responsabile del trattamento, in quanto una eventuale inerzia del secondo causerebbe un responsabilità del primo.

È opportuno, pertanto, che la materia sia oggetto di specifiche discipline contrattuali nell'accordo tra titolare e responsabile, prevedendo termini ridottissimi per il flusso di informazioni da responsabile a titolare quanto a verificarsi del data breach:

> *"the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours".*

Si suggerisce una clausola del seguente tenore

> *"Il RdT è obbligato a dare immediata notizia al TdT di ogni violazione della sicurezza da cui possa derivare una violazione dei dati personali. Si considera immediata la notizia pervenuta al più tardi entro (12) ore dalla presa di conoscenza iniziale, fatto salvo ogni ulteriore attività istruttoria. La violazione della prescrizione costituisce causa espressa di risoluzione del contratto, fatto salvo il risarcimento del danno"*

4.ARRICCHIMENTO DELLA NOTIZIA

La piena consapevolezza dell'intervenuta violazione della sicurezza con conseguente violazione dei dati potrebbe raggiungersi solo a seguito di idonea istruttoria.

Le ragioni dell'istruttoria dettagliata e analitica possono confliggere, in concreto, con l'esigenza di celerità del procedimento di disclosure del data breach.

IL RGPD ammette solo uno short period of investigation, condotta, magari, da un'unità aziendale di crisi, all'esito del quale passare a una scelta in un senso o nell'altro:

> *"After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware".*

In ogni caso bisogna lasciare traccia documentale anche nel caso non si proceda alla notificazione, dando le motivazione di tale opzione negativa:

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented.

Altrettanto è a dirsi per l'ipotesi di superamento del termine di 72 ore: bisogna lasciare traccia della giustificazione delle ragioni della dilazione.

5. NOTIFICA DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

Altro quesito pratico è se la notificazione della violazione dei dati possa essere delegata al Rdt.

La risposta non sta nella disciplina espressa del Regolamento, ma può derivare dai principi generali.

Per contratto, infatti, il RdT potrebbe essere investito del compito di effettuare, in nome e per conto del TdT, la notificazione suddetta.

Tale delega contrattuale ha valore tra le parti, ma non comporta mai una deresponsabilizzazione del TdT.

Si sottolinea, a tale proposito, che omissioni, ritardi e inadeguatezza della notificazione sono circostanza che verranno comunque poste a carico del TdT, senza che si possa opporre all'Autorità di controllo l'avvenuto conferimento di delega al RDT:

"A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller."

6. REGISTRO DELLE VIOLAZIONI

Il Regolamento 2016/679 non fa un richiamo testuale, ma è opportuno che il TdT si doti di un registro delle violazioni, nel quale annotare le violazioni della sicurezza. Sarà, questo, il documento in cui si censiscono sia le violazioni notificate all'Autorità di controllo, sia le violazioni non notificate.

Il registro deve essere mantenuto a disposizione dell'Autorità di controllo, per l'ipotesi di attività di indagine della stessa. Il termine di conservazione del registro delle violazioni deve essere determinato dallo stesso Tdt:

"The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data and to meet a lawful basis for processing."

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

7. COMUNICAZIONI AGLI INTERESSATI

Per le Comunicazioni agli interessati le Linee Guida del WP29 indicano i seguenti mezzi: posta elettronica, sms, messaggi diretti, banner, Comunicazioni postali, annunci sulla stampa.

Bisogna comunque scegliere uno strumento o più strumenti combinati tra loro, che massimizzino le possibilità di conoscenza, nei casi in cui non sia proceda con comunicazioni individuali:

> *A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.*

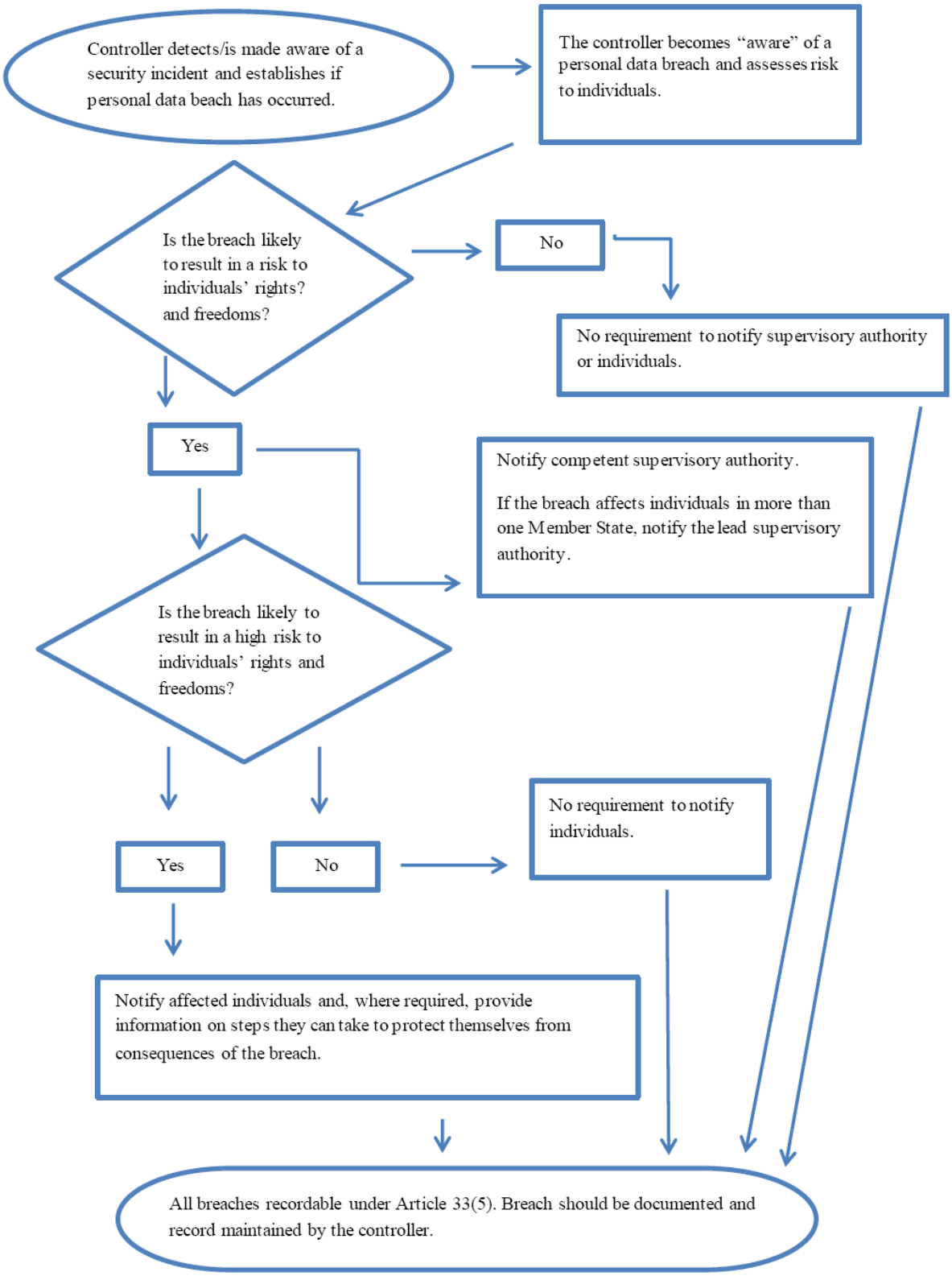
FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

8. CASISTICA

Esempi	Notificare ad Autorità di Controllo?	Comunicare agli Interessati?	Raccomandazioni
1. Un Titolare del Trattamento ha conservato una copia di un archivio di dati personali criptati su un CD. Il CD viene rubato.	No.	No.	Finché 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 membro	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.	
3. Un breve blackout, 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 dati 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 vigilanza 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. 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.	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.
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 può 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). I titolari del trattamento devono quindi informare l'autorità di vigilanza.	Se non ci sono alti rischi per i singoli interessati, essi non devono essere notificati.	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.
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, notificare 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, notificare 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, notificare 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.

FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**

9. IL FLUSSO DEL DATA BREACH (Fonte WP29 versione inglese)



FEDERPRIVACY – Associazione Professionale ai sensi della Legge 4/2013, iscritta nel Registro del Ministero dello Sviluppo Economico - Sede: Via Degli Innocenti, 2 – 50063 Figline Valdarno (FIRENZE) ITALY - Codice Fiscale 94156260484 - Partita Iva IT06413480481 – Tel. +39 055 5276058 – **Numero Verde 800910424** – Fax +39 055 5609184 - Web: **www.federprivacy.org** - Email: **info@federprivacy.it** - Pec: **federprivacy@pec.it**- Skype: **Federprivacy** - Twitter: **@Federprivacy**