PROCEDURA RELATIVA ALLA NOTIFICA DI VIOLAZIONE SUI DATI PERSONALI (DATA BREACH)

La presente procedura stabilisce gli adempimenti da porre in essere nel caso di violazioni dei dati personali trattati dal Titolare conformemente alle previsioni dalla normativa privacy vigente.

PREMESSE

Il Collegio, in qualità di Titolare del trattamento (di seguito anche "Titolare del trattamento"), è tenuto ai sensi del Regolamento Europeo 2016/679 (di seguito anche "GDPR") a mantenere sicuri i dati personali trattati dalla propria struttura e a reagire senza ingiustificato ritardo in caso di violazione dei dati personali (incluse eventuali notifica all'Autorità Garante competente ed eventuali comunicazioni agli interessati).

È di fondamentale importanza predisporre azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali, al fine di evitare rischi per i diritti e le libertà degli interessati, nonché danni economici all'azienda, che permettano, altresì di rispettare gli adempimenti previsti dalla normativa europea, nei tempi e modi ivi previsti (es. notificazione all'autorità garante e/o comunicazione agli interessati).

Le sanzioni previste dal GDPR per omessa notifica di Data Breach all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo al Titolare di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del fatturato di Gruppo annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 c. 2.

SCOPO

Lo scopo di questa procedura è di fornire un flusso di gestione delle violazioni dei dati personali trattati dal Titolare. Questo documento integra le procedure in essere presso il Titolare del trattamento ai sensi del GDPR e degli ulteriori provvedimenti in materia di protezione dei dati personali.

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Una violazione di dati personali è ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare del trattamento.

Le violazioni di dati personali possono accadere per un ampio numero di ragioni, che possono includere:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico;
- accesso abusivo: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite;
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (i.e. forzatura di porte o finestre di stanze di sicurezza o archivi contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

Il WP29 (Gruppo di Lavoro Articolo 29), nel suo parere n. 3 del 2014, ha classificato le violazioni in base ai seguenti tre ben noti principi di sicurezza delle informazioni:

- Violazione della riservatezza: in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- Violazione della disponibilità: in caso di perdita non autorizzata o accidentale o in caso di distruzione di dati personali;
- Violazione dell'integrità: in caso di alterazione non autorizzata o accidentale dei dati personali.

AMBITO DI APPLICAZIONE E DESTINATARI

Questa procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento (meglio descritti al punto 5 della presente procedura) quali:

- tutti i lavoratori dipendenti, nonché a coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento (di seguito genericamente denominati DESTINATARI INTERNI);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dal DESTINATARIO INTERNO che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare (di seguito genericamente denominati DESTINATARI ESTERNI);

di seguito, genericamente denominati "DESTINATARI".

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento, **senza indebiti ritardi** e, ove possibile, **entro 72 ore dalla scoperta**, deve notificare la violazione al Garante per la protezione dei dati personali, **a meno che sia improbabile** che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro**. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

A QUALI TIPI DI DATI SI RIFERISCE QUESTA PROCEDURA

Queste procedure si riferiscono a:

- dati personali trattati da e per conto del Titolare del trattamento, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo (i.e. sistemi informatici);
- dati personali conservati o trattati a mezzo di qualsiasi altro sistema aziendale.

Per «dato personale» si intende "qualsiasi informazione riguardante una persona fisica identificata o

identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

GESTIONE DELLA COMUNICAZIONE INTERNA DI DATA BREACH

Le violazioni di dati personali aventi natura tecnologica e la violazione a livello cartaceo sono gestite dal Titolare con il supporto dell'Amministratore di Sistema ove nominato. In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa sia affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione e prevenire che si ripeta.

Nel caso in cui uno dei DESTINATARI si accorga di una concreta, potenziale o sospetta violazione dei dati personali, dovrà immediatamente **informare dell'incidente il Presidente e, per conoscenza, l'Amministratore di sistema se nominato mediante la compilazione dell'Allegato A – Modulo di comunicazione interna di Data Breach da inviare a mezzo mail all'indirizzo vicenza@cng.it o all'indirizzo personale del Presidente presidente@geometri.vi.it. Per conoscenza, dovrà essere informato anche il Responsabile Protezione Dati (RPD) nella figura del Referente**: Avv. Margherita Patrignani del Foro di Rimini, con Studio in Cattolica (RN), Via S. Allende n. 99, casella di posta elettronica dedicata E-mail rpdgeometri@compliancelegaleservizi.com

GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

Nella gestione della notizia della violazione di dati personali pervenuta il Titolare dovrà seguire i seguenti cinque step:

Step 1: Identificazione e indagine preliminare

L'Allegato A permetterà al Titolare di condurre una valutazione inziale della notizia dell'incidente occorso, per stabilire se sia effettivamente accaduto un Data Breach (violazione) e se sia necessaria un'indagine più approfondita dell'accaduto, procedendo con il risk assessment (step 2).

Infatti, mentre tutte le violazioni di dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali (es. un incidente che porta alla indisponibilità dei dati personali per un certo periodo di tempo è una violazione della sicurezza, che dovrà essere documentata attraverso l'inserimento nell'Allegato B - Registro delle violazioni, tuttavia a seconda delle circostanze può o meno richiedere la notifica all'Autorità di Controllo e la comunicazione agli individui interessati. Se la mancanza di disponibilità dei dati personali può comportare un rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento dovrà effettuare notifica).

Detta valutazione iniziale sarà effettuata attraverso l'esame delle informazioni riportate nell'Allegato A:

- La data di scoperta della violazione (tempestività);
- Il soggetto che è venuto a conoscenza della violazione;

- Breve descrizione dell'incidente (natura della violazione e dei dati coinvolti);
- Le categorie, il numero approssimativo di interessati coinvolti nella violazione e di registrazioni di dati personali in questione;
- Breve descrizione di eventuali azioni già poste in essere.

Step 2: Contenimento Recovery e Risk assessment

Una volta stabilito che un Data Breach è avvenuto, il Titolare dovrà stabilire:

- Se esistono azioni che possano limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di strumentazione; l'utilizzo dei file di back up per recuperare dati persi o danneggiati; isolando/chiudendo un settore compromesso della rete; cambiando codici di accesso delle entrate; ecc.);
- Una volta identificate tali azioni, quali siano i soggetti che devono agire per contenere la violazione;
- **Se sia necessario notificare la violazione all'Autorità Garante per la Protezione dei dati personali** (ove sia probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche);
- Se sia necessario comunicare la violazione agli interessati (ove la violazione presenti un elevato rischio per i diritti e le libertà delle persone fisiche).

Per determinare la necessità di notificazione all'Autorità Garante e di comunicazione agli interessati, **il Titolare determinerà la gravità della violazione utilizzando lo strumento di autovalutazione (self assessment), messo a disposizione dal Garante alla pagina** https://servizi.gpdp.it/databreach/s/self-assessment che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza, esaminandolo insieme con l'Allegato A e tenendo in debita considerazione i principi e le indicazioni di cui all'art. 33 GDPR e valutando i rischi per i diritti e le libertà delle persone fisiche.

Se, infatti, gli obblighi di notifica all'Autorità di Controllo scaturiscono dal superamento di una soglia di rischio semplice, l'art. 34 GDPR prevede invece che l'obbligo di comunicazione agli interessati sia innescato dal superamento di un rischio elevato.

In calce sono indicati degli esempi di data breach con valutazione di gravità.

Step 3: Eventuale notifica all'Autorità Garante competente

Una volta valutata la necessità di effettuare notifica della violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, **il Titolare dovrà provvedervi, senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza**.

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali; ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la

discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

La notifica deve contenere almeno le informazioni sinteticamente riportate in questa pagina (art. 33, par. 3 del Regolamento (UE) 2016/679):

- una descrizione della natura della violazione dei dati personali, che comprenda, se possibile:
- le categorie e il numero approssimativo di persone interessate;
- le categorie e il volume approssimativo di dati personali interessati;
- il nome e i riferimenti di contatto del responsabile della protezione dei dati (se designato dal titolare) o comunque di un referente competente a fornire informazioni;
- una descrizione delle possibili conseguenze della violazione dei dati personali;
- una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi;
- SOLO in caso di notifica effettuata oltre il termine prescritto di 72 ore, una descrizione dei motivi del ritardo.

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (Provvedimento del 27 maggio 2021).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza, come indicato al paragrafo precedente.

Step 4: Eventuale comunicazione agli interessati

Una volta valutata la necessità di effettuare comunicare agli interessati la violazione dei dati subita sulla base della procedura di cui allo step 2, secondo quanto prescritto dal Regolamento (UE) 2016/679, il Titolare dovrà provvedervi, senza ingiustificato ritardo.

Quanto al contenuto di tale comunicazione, il Titolare dovrà fare attenzione almeno ai seguenti aspetti:

- comunicare il nome e i dati di contatto del responsabile della protezione dei dati (DPO) 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.

Quanto alle modalità di comunicazione, caso per caso, si dovrà sempre privilegiare modalità di comunicazione diretta con i soggetti interessati (quali e-mail, SMS o messaggi diretti). Il messaggio dovrà essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di update generali o newsletter, che potrebbero essere facilmente fraintesi dai lettori. Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica (quale un alert sul sito internet istituzionale), che dovrà essere ugualmente efficace nel contatto diretto con l'interessato.

Step 5: Documentazione della violazione

Indipendentemente dalla valutazione circa la necessità di procedere a notificazione e/o comunicazione della violazione di Data Breach, ogni qualvolta si verifichi un incidente comunicato dai DESTINATARI attraverso l'Allegato A, il Titolare sarà tenuta a documentarlo.

Tale documentazione sarà affidata al Titolare, che vi provvederà mediante la tenuta dell'**Allegato B - Registro dei Data Breach**, secondo le informazioni ivi riportate: (i) n. violazione; (ii) data violazione; (iii) natura della violazione; (iv) categoria di interessati; (v) categoria di dati personali coinvolti; (vi) numero approssimativo di registrazioni dei dati personali; (vii) conseguenze della violazione; (viii) contromisure adottate; (ix) se sia stata effettuata notifica all'Autorità Garante Privacy; (x) se sia stata effettuata comunicazione agli interessati.

Il Registro dei Data Breach deve essere continuamente aggiornato, firmato digitalmente dal Presidente per conferire data certa e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

*

Documento aggiornato al 27/05/2024 *Firma del Titolare del Trattamento* Daniele Fortuna

*

Allegato A: MODULO DI COMUNICAZIONE INTERNA DI DATA BREACH

Da compilare a cura dei Destinatari (interni e esterni) e da inviare al Titolare e, per conoscenza, all'Amministratore di sistema, se presente, e al RPD, se nominato, come da paragrafo 6 della presente procedura.

Comunicazione di Data Breach	**Note**
Data scoperta incidente:	

Data dell'incidente:	
Nome cognome e dati di contatto (indirizzo e-mail, numero telefonico) della persona che compila il presente modulo. In caso di destinatario esterno indicare anche la ragione sociale:	
Luogo dell'incidente (se in Italia o all'estero e specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili):	
Breve descrizione dell'incidente (con precisazione della natura della violazione: violazione della riservatezza; violazione della disponibilità; violazione dell'integrità):	
Breve descrizione della/e banca/che dati oggetto dell'incidente e della tipologia di dati coinvolti (es. dati personali comuni; categorie particolari di dati, tra cui origine razziale o etnica, opinioni politiche, convinzioni religiose, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale; dati relativi a condanne penali e reati):	
Categorie (es. lavoratori; clienti; fornitori; utenti sito web) e numero approssimativo di interessati coinvolti nell'incidente e numero approssimativo di registrazioni dei dati personali coinvolti:	
Breve descrizione di eventuali azioni poste in essere al momento della scoperta dell'incidente:	
Responsabile del settore di appartenenza/Referente interno:	
Data:	

*

Allegato B: REGISTRO DELLE VIOLAZIONI

Si riporta un facsimile del registro delle violazioni da compilare a cura del Titolare a seconda della natura della stessa.

N° violazione	Data violazione	Natura della violazione	Categoria di interessati	Categoria di dati perosnali coinvolti	Numero approssimativo di registrazioni dei dati personali	Conseguenze della violazione	Contromisure adottate	E' stata effettuata notifica all'Autorità Garante privacy?	E' stata fatta comunicazione agli interessati?

*

Esempi di violazioni dei dati personali, non esaustivi, che aiuteranno il Titolare ("controllore") a distinguere tra basso rischio e alto rischio per i diritti e le libertà degli individui e a determinare la necessità dell'eventuale notifica al Garante e ai soggetti interessati.

ESEMPIO	NOTIFICARE ALL'AUTORITÀ DI VIGILANZA?	NOTIFICARE AI SOGGETTI INTERESSATI?	NOTE/RACCOMANDAZIONI

1. un controllore ha memorizzato una copia di backup di un archivio di dati personali criptati su una chiavetta USB. La chiave viene rubata durante un'effrazione.	No	No	Fintanto che i dati vengono crittografati con uno stato dell'algoritmo dell'arte, i backup dei dati esistenti la chiave univoca non è compromessa, e i dati possono essere ripristinati in tempo utile, questo non può essere una violazione segnalabile. Tuttavia, se viene successivamente compromessa, è richiesta la notifica.
2. un controllore gestisce un servizio online. Come risultato di un attacco cibernetico su tale servizio, i dati personali degli individui sono trafugati. Il controllore ha clienti in un unico Stato membro.	Sì, riferire all'autorità di vigilanza se ci sono probabili conseguenze per gli individui.	Sì, riferisca agli individui secondo la natura dei dati personali influenzati e se la severità delle conseguenze probabili agli individui è alta.	
3. una breve interruzione di corrente della durata di alcuni minuti presso il Call Center di un controller significa che i clienti non possono chiamare il controllore e accedere ai loro record.	No	No	Questa non è una violazione denunciabile, ma ancora un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. I record appropriati devono essere mantenuti dal controllore.
4. un controllore soffre di un attacco ransomware che si traduce in tutti i dati crittografati. Non sono disponibili Back-UPS e i dati non possono essere ripristinati. In materia di indagine, diventa chiaro che il ransomware solo la funzionalità era quella di criptare i dati, e che non c'era altro malware presente nel sistema.	Sì, riferire all'autorità di vigilanza, se ci sono probabili conseguenze per gli individui in quanto si tratta di una perdita di disponibilità.	Sì, relazione agli individui, a seconda della natura dei dati personali interessati e il possibile effetto della mancanza di disponibilità dei dati, così come altri probabili Conseguenze.	Se fosse disponibile un backup e i dati potessero essere ripristinati in tempo utile, ciò non avrebbe bisogno di essere denunciato all'autorità di vigilanza o alle persone in quanto non vi sarebbe stata alcuna perdita permanente di disponibilità o Riservatezza. Tuttavia, se l'autorità di vigilanza è venuta a conoscenza dell'incidente con altri mezzi, può prendere in considerazione un'inchiesta per valutare il rispetto dei requisiti di sicurezza più ampi dell'articolo 32.
5. un singolo telefono un Call Center di una banca per segnalare una violazione dei dati. L'individuo ha ricevuto una dichiarazione mensile per qualcun altro. Il controllore si assume una breve indagine (cioè completato entro 24 ore) e stabilisce con una ragionevole fiducia che una violazione dei dati personali si è verificato e se ha un difetto sistemico che può significare altri individui sono o potrebbero essere colpiti.	Sì	Solo gli individui colpiti sono informati se c'è un rischio elevato ed è chiaro che altri non sono stati colpiti.	Solo gli individui colpiti sono informati se c'è un rischio elevato ed è chiaro che altri non sono stati colpiti.

6. un controllore gestisce un mercato online e dispone di clienti in più Stati membri. Il Marketplace soffre di un cyber-attacco e nomi utente, le password e la storia di acquisto sono pubblicate on-line da parte dell'aggressore.	Sì, riferisca di dirigere l'autorità di sorveglianza se coinvolge l'elaborazione transfrontaliera.	Sì, come potrebbe portare ad un rischio elevato.	Il controllore dovrebbe agire, ad esempio forzando le reimpostazioni delle password degli account interessati, nonché altri passaggi per attenuare il rischio. Il controllore dovrebbe inoltre prendere in considerazione qualsiasi altro obbligo di notifica, ad esempio sotto la direttiva NIS come fornitore di servizi digitali.
7. una società di Web hosting che funge da processore di dati identifica un errore nel codice che Controlla l'autorizzazione dell'utente. L'effetto del difetto significa che qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	Come il processore, il sito web società di hosting deve informare i suoi clienti interessati (i controllori) senza ritardo indebito. Supponendo che la società di hosting sito ha condotto la propria indagine i controllori interessati dovrebbero essere ragionevolmente fiduciosi se ciascuno ha subito una violazione e quindi rischia di essere considerato come avente "prendere coscienza" una volta che sono stati notificato dalla società di hosting (il processore). Il controllore deve quindi notificare all'autorità di vigilanza.	Se non vi è probabilmente alcun rischio elevato per gli individui non hanno bisogno di essere Notificato.	Il sito Web Hosting Company (processore) deve prendere in considerazione eventuali altri obblighi di notifica (ad esempio, sotto il NIS Direttiva come fornitore di servizi digitali). Se non vi sono prove di sfruttamento di questa vulnerabilità con uno dei suoi controllori, non può essersi verificata una violazione di notifica, ma è probabile che sia registrabile o sia una questione di non conformità ai sensi dell'articolo 32.
8. cartelle cliniche in un ospedale non sono disponibili per il periodo di 30 ore a causa di un cyber-attacco.	Sì, l'ospedale è obbligato a notificare come ad alto rischio per il benessere del paziente e la privacy può verificarsi.	Sì, riferire agli individui colpiti.	
9. i dati personali di un gran numero di studenti vengono erroneamente inviati alla mailing list sbagliata con 1000 + destinatari.	Sì, riferisca all'autorità di vigilanza.	Sì, riferire agli individui a seconda della portata e del tipo di dati personali coinvolti e la gravità delle possibili conseguenze.	
10. una e-mail di direct marketing viene inviata ai destinatari nei campi "a:" o "CC:", consentendo in tal modo a ciascun destinatario di visualizzare l'indirizzo email di altri destinatari.	Sì, notificando l'autorità di vigilanza può essere obbligatorio se un gran numero di individui sono interessati, se i dati sensibili sono rivelati (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio la posta contiene le password iniziali).	Sì, riferire agli individui a seconda della portata e del tipo di dati personali coinvolti e la gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se vengono rivelati solo un numero minore di indirizzi e-mail.