Cosa fare nel caso in cui i dati personali vengano violati ?
(c.d. «*Data Breach*»)

- **NOTIFICA** all'Autorità di Controllo (art. 33)

Quando? Sempre, a meno che sia ''improbabile'' che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. [Secondo quindi una valutazione rispondente ad un concetto (''impossibilità'') ancora assai indeterminato].

- **COMUNICAZIONE** all'interessato (art. 34)

Quando? Se la violazione è suscettibile di presentare un rischio ''**elevato**'' per i diritti e le libertà delle persone fisiche e **non** si rientri in uno dei tre casi previsti dal terzo comma (cfr. Slide 7). [Secondo, quindi, nuovamente, una valutazione ad oggi poco compatibile con il principio di determinazione].

NOTIFICA all'Autorità

Art. 33, comma 1

«*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55* ***senza ingiustificato ritardo*** *e, ove possibile,* ***entro 72 ore dal momento in cui ne è venuto a conoscenza****, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei* ***motivi del ritardo***». [Nuovamente valutazioni che, nell'attuale assenza di regolamenti, codici di condotta, *guide-lines**, sono di difficile interpretazione].

Art. 33, comma 2

«*Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione*».

_____

* Il Gruppo di lavoro istituito dall'art. 29 della Direttiva 46/1995 (e destinato ad essere sostituito dal Comitato europeo per la protezione dei dati *ex* artt. 68 e seg. GDPR) ha iniziato ad elaborare alcune Linee Guida esplicative che potranno fungere da punto di partenza per una più compiuta lettura delle norme.

Contenuto essenziale della NOTIFICA:

- 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 (DPO) 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.

L'istituto della «Notifica» all'Autorità non è nuovo. Il Codice della Privacy prevedeva infatti:

- una COMUNICAZIONE «*senza indebiti ritardi*» al Garante in caso di *data breach*, imposta però al solo «***fornitore di servizi di comunicazione elettronica*** *accessibili al pubblico*» (es. reti internet e telefoniche). Il GDPR la impone invece a **tutti** i Titolari del trattamento;

- una NOTIFICAZIONE **preventiva** al Garante concernente il trattamento di dati personali cui il titolare intende procedere. Il GDPR ha eliminato il dovere di comunicare *ex ante* i trattamenti di dati cui si intende dar corso, sostituendolo con l'obbligo di procedere ad una ***Valutazione d'impatto*** del trattamento sulla protezione dei dati.

VALUTAZIONE DI IMPATTO (art. 35)

Nel caso in cui il trattamento di dati preveda l'uso di «*nuove tecnologie*» e presenti un «*rischio elevato*» per i diritti e le libertà delle persone fisiche, prima di procedere a tale trattamento il Titolare ne valuta i potenziali effetti sulla protezione che deve essere assicurata ai dati personali.

Ove la Valutazione di impatto indichi che, in assenza di specifiche misure tecniche adottate, il trattamento potrebbe presentare un rischio elevato, il Titolare effettua una CONSULTAZIONE PREVENTIVA (art. 36) dell'Autorità di controllo. Questa fornirà al Titolare un parere scritto indicando le più opportune modalità e misure tecniche da adottare (cfr. Slide 14 – Poteri consultivi dell'Autorità).

In breve:

In ossequio ai principi di «*accountability*» e di «responsabilizzazione», il GDPR non impone più un generale obbligo di informare preventivamente l'Autorità prima di procedere al trattamento di dati personali, ma investe il Titolare dell'onere di valutare «caso per caso» la rischiosità di determinati trattamenti, lasciando che sia quest'ultimo a decidere sull'opportunità di consultare l'Autorità prima di procedere al trattamento. [Necessità di percorsi ''motivazionali'' documentati e trasparenti].

Dall'altro lato, l'obbligo di notificare l'Autorità in caso di *data breach* non è più rivolto al solo «fornitore di servizi di comunicazione elettronica», ma viene genericamente esteso a tutti i Titolari del trattamento [che possono essere persone giuridiche].

COMUNICAZIONE all'interessato

E' dovuta quando il *data breach* sia suscettibile di presentare un rischio **elevato** [?] per i diritti e le libertà delle persone fisiche, **a meno che** non si incorra in uno dei seguenti casi:

a) il titolare del trattamento ha messo in atto misure di protezione tecniche ed organizzative adeguate [?] e tali misure erano state applicate ai dati personali oggetto della violazione. Si tratta in particolare delle misure destinate a rendere i dati incomprensibili per chi non sia autorizzato ad accedervi (es. 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.

Contenuto essenziale della COMUNICAZIONE all'interessato:

La comunicazione deve descrivere con un **linguaggio semplice** e **chiaro** la natura della violazione e deve contenere quantomeno le seguenti informazioni:

a) 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;
b) **probabili conseguenze** [?] della violazione dei dati personali;
c) **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.

QUADRO SANZIONATORIO

Il GDPR dispone che i trattamenti illeciti di dati personali siano sanzionati su tre piani:

- **AMMINISTRATIVO**: severe sanzioni pecuniarie (in buona parte già previste, ma che potranno essere implementate dai singoli Stati membri) [maggior compatibilità con la sanzionabilità di una persona giuridica e non fisica];

- **CIVILE**: legittimazione dell'interessato ad agire nei confronti del Titolare e del Responsabile per il ristoro del danno patito;

- **PENALE**: fattispecie e sanzioni ancora non definite. La loro predisposizione spetta ai singoli legislatori nazionali. [Problemi di compatibilità con: *a)* responsabilità personale; *b) bis in idem*; *c)* principio *nemo tenetur se detegere*; *d)* coordinamento con D.lgs. 231/01; *e)* concorso con reato di ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza *ex* art. 2638 c.c.]

SANZIONI AMMINISTRATIVE (art. 83)

A seconda del tipo di violazione sono previste due cornici sanzionatorie:

1) fino a € 10 milioni o, per le imprese, **fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente (se superiore), nel caso in cui in cui la violazione abbia ad oggetto:

- gli obblighi del titolare o del responsabile del trattamento previsti dagli artt. 8 (condizioni del consenso del minore), 11 (trattamento che non richiede identificazione), 25 – 39 (*privacy by design* e *by default*; norme su Titolare e Responsabile; registro attività di trattamento; notifiche e comunicazioni di *data breach*; valutazione d'impatto; norme sul DPO), 42 e 43 (certificazione ed organismo di certificazione);
- gli obblighi dell'organismo di certificazione a norma degli artt. 42 e 43;
- gli obblighi dell'organismo di controllo a norma dell'art. 41, comma 4.

SANZIONI AMMINISTRATIVE (*segue*)

2) fino a € 20 milioni o, per le imprese, **fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente (se superiore), nel caso in cui la violazione abbia ad oggetto:

- i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli artt. 5 (principi applicabili al trattamento), 6 (liceità del trattamento), 7 (condizioni per il consenso) e 9 (trattamento di dati c.d. "sensibili");
- i diritti degli interessati ai sensi degli artt. 12 – 22;
- il trasferimento di dati personali ad un destinatario in un paese terzo o ad un'organizzazione internazionale *ex* artt. 44 – 49;
- qualsiasi obbligo ai sensi delle legislazioni dei singoli Stati membri adottate a norma del capo IX;
- l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati emanato dall'Autorità di controllo *ex* art. 58, comma 2, o il negato accesso *ex* art. 58, comma 1. (cfr. Slide 15 – Poteri di indagine delle Autorità)

NORME DI CHIUSURA DELL'APPARATO SANZIONATORIO

L'art. 84 si pone quale "norma di chiusura" dell'apparato sanzionatorio del GDPR, affermando che

«*gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni* ***non*** *soggette a sanzioni amministrative pecuniarie a norma dell'art. 83* […]*. Tali sanzioni devono essere effettive, proporzionate e dissuasive*».

[Legge delega 25 ottobre 2017, n. 163 che prescrive al Governo di adottare, «***entro sei mesi*** *dall'entrata in vigore della presente legge,* […] *uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del regolamento (UE) 2016/679*»].

Quest'ultima previsione necessita di lettura combinata a quella del *considerandum* n. 149, secondo il quale

«*Gli Stati membri* ***dovrebbero*** *poter stabilire* […] ***sanzioni penali*** *per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento*». Si precisa poi che l'imposizione di sanzioni penali e amministrative «*non dovrebbe essere in contrasto con il principio del* ***ne bis in idem*** *quale interpretato dalla Corte di giustizia*».

TRE OPZIONI PER IL LEGISLATORE **PENALE** NAZIONALE

1. abrogare le fattispecie penali attualmente vigenti (previste dal Cod. Privacy) ed introdurre nuove fattispecie penali conformi al GDPR;

2. abrogare le fattispecie penali attualmente vigenti (previste dal Cod. Privacy) ed introdurre nuove sanzioni amministrative;

3. riformulare le fattispecie penali attualmente vigenti nelle sole parti incompatibili con il GDPR.

POTERI DELLE AUTORITA' DI CONTROLLO (art. 58)

I poteri attribuiti alle Autorità di controllo possono ricondursi a tre distinte macro-categorie:

- poteri di **INDAGINE**

(*cfr. slide successiva*)

- poteri **CORRETTIVI**

(es. rivolgere ammonimenti a Titolare e Responsabile che abbiano violato il Regolamento, nonché quello di ingiungere al Titolare di comunicare all'interessato una violazione che abbia interessato i suoi dati personali)

- poteri **AUTORIZZATIVI** e **CONSULTIVI**

(es. quelli esercitati per orientare l'agire del Titolare a seguito di Valutazione di impatto negativa)

* * *

N.B. Ad ogni Paese viene rimessa la facoltà di riconoscere alla/e propria/e Autorità di controllo **poteri ulteriori** rispetto a quelli già previsti dal Regolamento. In Italia l'Autorità di controllo non è ancora stata ufficialmente designata. Nelle more questa viene dunque ad essere identificata col Garante della Privacy (che si sta in parte facendo carico dei compiti propri dell'Autorità *ex* art. 57)

POTERI DELLE AUTORITA' DI CONTROLLO (*segue*)
- Poteri di **INDAGINE** -

Tra i poteri di indagine riconosciuti alle Autorità di Controllo bene ricordare i principali:

- **ingiungere** al Titolare, al Responsabile del trattamento e, ove applicabile, al loro Rappresentante, **di fornirle ogni informazione di cui necessiti** per l'esecuzione dei suoi compiti;

- **condurre indagini** sotto forma di attività di revisione sulla protezione dei dati;

- **ottenere**, dal Titolare o dal Responsabile del trattamento, **l'accesso a tutti i dati personali e a tutte le informazioni necessarie** per l'esecuzione dei suoi compiti;

- **ottenere accesso a tutti i locali** del Titolare e del Responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, **in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri**