Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

ORDINE DEGLI AVVOCATI DI TORINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Tavolo di lavoro congiunto "Protezione dei dati personali – GDPR

Data breach: prevenire è meglio che curare

Riflessi su professionisti e PMI

a cura del Referente del TdL congiunto «Protezione dei dati personali – GDPR»
Ordine dei Dottori Commercialisti ed Esperti Contabili di Torino

Paola Zambon *Dottore Commercialista*

Torino, 14 maggio 2021

PREMESSA METODOLOGICA

Quando si utilizza il termine «Professionista» si intende per questa presentazione:

Dottore Commercialista, Esperto Contabile, Avvocato, Ingegnere

Poiché la tesi riportata è stata coordinata nel Tavolo di lavoro congiunto «Protezione dei dati personali – GDPR»

Tavolo di lavoro congiunto «Protezione dei dati personali – GDPR»

TaxLawPlanet™

TAVOLO CONGIUNTO GDPR ORDINI PROFESSIONALI DI TORINO

Gli Ordini dei **Dottori Commercialisti** ed Esperti Contabili, degli **Avvocati** e degli **Ingegneri** di Torino,

hanno lavorato assieme per affrontare al meglio il cammino verso il GDPR

Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

ORDINE DEGLI AVVOCATI DI TORINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TORINO

Un supporto per le nostre Categorie

- Evidenziare l'importanza della norma sensibilizzando in particolare sugli effetti della «responsabilizzazione»
- Informare e formare i Professionisti nei propri studi professionali
- Offrire spunti utili per impostare i propri lavori e suggerimenti applicativi
- Invitare i colleghi che hanno maturato esperienza in materia di protezione dei dati personali a proseguire nella loro attività dedicando una particolare attenzione all'auto-formazione
- Essere di riferimento verso le Autorità competenti

TaxLawPlanet™

Data breach al sito del ministero della Giustizia: in chiaro i dati personali di candidati all'esame di avvocato

Esame di Stato per l'esercizio della professione di Avvocato

Ministero della Giustizia

Home candidato

Elenco delle domande di partecipazione

Comunicazioni per il candidato
Comunicazioni dalla Corte di Appello
Modifica i dati della registrazione (Storico modifiche)

(Storico modifiche domanda)
Accesso Atti
Materie prove orali o rinuncia

Esame per Avvocati

Attualmente non è presente alcun concorso attivo per cui presentare o modificare una domanda.

Hai già inviato una domanda di partecipazione per la sessione corrente.
Selezionare il collegamento seguente per scaricare il modulo per la marca da bollo : Scarica il modulo (.pdf)

UID	Data compilazione	Cognome	Nome	Corte di appello	Stato	Azioni
[redacted]	02/10/2020 12:26:25	[redacted]	VALENTINA	Corte di Appello Milano	INVIATA	Scarica la domanda di partecipazione (.pdf) Scarica il codice identificativo (.pdf)

Se hai problemi, scarica il manuale on-line

© Ministero della Giustizia - v2.4

https://www.cybersecitalia.it/data-breach-al-sito-del-ministero-della-giustizia-in-chiaro-i-dati-personali-di-candidati-allesame-di-avvocato/11294/

Per disporre di tutte le informazioni utili alla procedura accedere ai servizi dal sito Giustizia.it

Servizio in fase di ripristino, per informazioni scrivere a:

supportotecnicoutenti.siticoncorsiesami@giustizia.it

Principi di base di sicurezza e data breach

I dati personali devono essere «**trattati in maniera da garantire un'adeguata sicurezza dei dati personali**, compresa la protezione, mediante **misure tecniche e organizzative adeguate**, da **trattamenti non autorizzati o illeciti** e dalla **perdita**, dalla **distruzione** o dal **danno accidentali** («integrità e riservatezza»).

Titolari e responsabili
sono chiamati
a trattare i dati personali in sicurezza
tenendo conto di
stato dell'arte, costi di attuazione, natura, oggetto, contesto, finalità del trattamento, probabilità di rischio per violazione diritti e libertà persone fisiche

NO sicurezza NO Party!

La mancata attuazione del GDPR **<u>solo per motivi economici non è una scusa plausibile</u>** dal punto di vista giuridico

Una valutazione sulla sicurezza del trattamento deve essere **sempre** effettuata

Privacy by design e by default + misure adeguate

Il titolare del trattamento e il responsabile del trattamento mettono in atto misure **tecniche e organizzative** adeguate **per garantire un livello di sicurezza adeguato** al rischio. Misure che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) **la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento**;
- c) **la capacità di ripristinare tempestivamente la disponibilità** e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una **procedura per testare, verificare e valutare regolarmente l'efficacia delle misure** tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La **manutenzione programmata** che implica un **indisponibilità temporanea** non è un data breach!

Materiale tratto da:
https://www.garanteprivacy.it/regolamentoue/databreach

Cosa è un «data breach»?

- Una **violazione di sicurezza** che comporta - 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.

I data breach sono incidenti di sicurezza

Esempi:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati **per cause accidentali o per attacchi esterni**, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

Violazioni di dati personali (Data Breach)

Natura della violazione	
Perdita di	**Conseguenze**
Confidenzialità	Diffusione/ accesso non autorizzato o accidentale
Disponibilità	Modifica non autorizzata o accidentale
Integrità	Impossibilità di accesso, perdita, distruzione non autorizzata o accidentale

Una violazione dei dati personali può compromettere:

- la riservatezza,
- l'integrità o
- la disponibilità di dati personali

o una loro combinazione

Causa della violazione		
Interna	intenzionale	accidentale
Esterna	intenzionale	accidentale
Sconosciuta		
Altre cause		

Materiale tratto da:
https://www.garanteprivacy.it/regolamentoue/databreach

Cosa fare in caso di «data breach»?

- Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, 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.

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

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

Cosa prendere in considerazione per valutare il rischio potenziale causato?

- tipo di violazione;
- natura, carattere sensibile e volume dei dati personali;
- facilità di identificazione delle persone fisiche;
- gravità delle conseguenze per le persone fisiche;
- caratteristiche particolari dell'interessato;
- caratteristiche particolari del titolare del trattamento;
- numero di persone fisiche interessate.

Quando il titolare viene «a conoscenza» del data breach?

Quando ne è «**ragionevolmente certo**» che si sia trattato di incidente di sicurezza che abbia compromesso dati personali.

Importanza del piano di prevenzione:
Avendo adottato le misure di protezione adeguate per stabilirlo con immediatezza, tenendo conto della natura e della gravità della violazione e delle sue conseguenze, potrà poi agire tempestivamente nel caso in cui sia necessario effettuare notifica e comunicazione agli interessati, nonché adottare misure appropriate.

Esempi di violazioni e stato di conoscenza

Fatto	Violazione
Perdita di chiavetta USB priva di crittografia e dove non sia possibile stabilire se le persone non autorizzate abbiano avuto accesso ai dati	Violazione di riservatezza e di disponibilità. Lo stato di conoscenza è immediato
Un terzo informa il titolare di avere ricevuto una mail per errore	Violazione di riservatezza Lo stato di conoscenza è immediato
Un criminale informatico viola il sistema del titolare e lo contatta per chiedergli il riscatto.	Violazione di riservatezza, disponibilità e integrità del dato. Lo stato di conoscenza scatta dopo la verifica che la comunicazione sia vera.
Il responsabile IT dell'azienda informa il titolare che ha registrato una violazione (attacco) da terzi	La violazione dipende dal tipo di attacco. Lo stato di conoscenza scatta dal momento in cui il responsabile IT abbia comunicato al titolare la violazione
Una breve interruzione di corrente ha impedito ai clienti di un call center di raggiungere il titolare e di accedere alle proprie registrazioni	Non è un data breach ma l'incidente va inserito nel registro

Si possono notificare tutte le violazioni subite complessivamente o separatamente?

- Il titolare può presentare una notifica cumulativa di tutte le violazioni che ha subito se riguarda **lo stesso tipo di trattamento dati personali, violati nello stesso modo in un determinato lasso di tempo considerabile breve**.
- Se si verificate violazioni inerenti tipi di trattamento diversi violati in modo diverso la notifica deve essere separata.

Accountability e «data breach»

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

COSA NOTIFICARE?

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

La notifica va inviata via pec o via mail al Garante

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.

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.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica deve contenere le informazioni previste all'art. 33, par. 3 del Regolamento (UE) 2016/679 e indicate nell'allegato al **Provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951)**.

Qualora si utilizzi per la notifica il **modello allegato al provvedimento**, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

Cosa deve contenere la comunicazione?

- La comunicazione agli interessati coinvolti deve fornire «con un linguaggio semplice e chiaro» **(senza ingiustificato ritardo)** :
- una descrizione della **natura della violazione**;
- il **nome** e **dati di contatto** del responsabile della protezione dei dati (RPD) o di altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle **probabili conseguenze della violazione** dei dati personali;
- una descrizione delle **misure adottate** o di cui si propone l'adozione **per porre rimedio alla violazione** e anche, se del caso, **per attenuare i possibili effetti negativi per gli interessati.**
- Una **consulenza specifica** alle persone fisiche **sul modo in cui proteggersi** dalle possibili conseguenze negative della violazione
- Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che **non devono essere inviati insieme ad altre informazioni**, quali newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

https://servizi.gpdp.it/databreach/s/self-assessment

Autovalutazione?

- Lo strumento, messo a disposizione dal Garante nel proprio sito, è da considerarsi esclusivamente quale ausilio al processo decisionale del titolare del trattamento e non rappresenta il pronunciamento dell'Autorità

- Una valutazione iniziale di rischio potenziale da violazione come parte di valutazione di impatto sulla protezione dei dati effettuata sul trattamento di dati personali effettuati potrebbe essere utilmente presa in considerazione come base per valutare la circostanza specifica.

t0

Il titolare viene informato di un incidente di sicurezza

tempo per indagare e capire se davvero vi è stata violazione

t1

stato di conoscenza

tempo per approfondire e capire se il trattamento comporta rischi

72 ore da t1

non riguarda dati personali

Non è un data breach

riguarda dati personali

comporta rischi per diritti e libertà delle persone

SI notifica

non comporta rischi per diritti e libertà delle persone

NO notifica
NO comunicazione

i rischi per diritti e libertà delle persone sono elevati

SI comunicazione alle persone interessate e se richiesto fornire informazioni sui provvedimenti da adottare

https://www.linkedin.com/groups/8617764

Gruppo in Linkedin

DATA PROTECTION'S CORNER

L'ANGOLO DELLA PROTEZIONE DEI DATI PERSONALI E DELLA PRIVACY

FREE SPEECH IN OPEN PLATFORM

ON DATA PROTECTION'S RIGHTS AND PRINCIPLES

AND ON PRIVACY

ACCOUNTABILITY…

Meglio prevenire le violazioni dei dati preparandosi in anticipo, poiché alcune conseguenze potrebbero essere irreversibili e documentare ciò che si è fatto è importante.

Invito al convegno gratuito con il Politecnico di Torino:

20 novembre 2021

www.ictdott.com

© *Paola Zambon*
info at ictdott.com

TaxLawPlanet™

Il «tavolo di lavoro congiunto GDPR» dei nostri Ordini Professionali è al fianco dei colleghi e onorato di essere utile anche a tutte le persone interessate

grazie