DOCUMENTAZIONE DI SISTEMA PRIVACY E PROTEZIONE DATI PERSONALI

EDIZIONE 2023-2024

Istruzione operativa : CM-DIP679-ComunicazioneCandidatiRET
Versione : Rif. : ALLEGATI A e B compilati dal TDT del soggetto Candidato
Ultima revisione : INCARICHI SOGGETTI PRIVACY INTERNI ED ESTERNI GDPR-EU/REG.2016/679

Il presente documento da corso agli adempimenti del cosiddetto GDPR "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" che dal 25 maggio 2018 è pienamente operativo.

COMUNICAZIONE E RICHIESTA DI INFORMAZIONI PER

SOGGETTO GIURIDICO CANDIDATO RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI – ISTRUZIONI E RICHIESTA DI INFORMAZIONI

CANDIDATO .....

Att. Titolare e Responsabile del Trattamento dei Dati ai sensi del regolamento UE 2016/679

pec: .....

Il Titolare del Trattamento dei dati si avvale delle vostre prestazioni sulla base di specifcio rapporto contrattuale in essere e pertanto, a tale titolo, la vostra azienda vine candidata al ruolo di "Responsabile del trattamento" e risulta soggetta, dal 25 maggio, a tutti gli obblighi, oneri, doveri e prerogative, previsti dal GDPR.

In questo contesto vi chiediamo pertanto di volerci trasmettere l'allegato A debitamente compilato e contenente tutte le informazioni necessarie per la corretta gestione dei rapporti in base alla citata normativa. Il conferimento dei dati è obbligatorio e non necessita di consenso. I dati saranno trattati per l'esecuzione dei compiti e delle prerogative previste dalla citata normativa e potranno essere comunicati e trasmessi alle Autorità di Controllo. Si prevede inoltre la pubblicazione dei dati essenziali ai fini della trasparenza e per garantire la corretta informazione agli interessati.

Poichè la normativa prevede una stretta collaborazione fra responsabile e titolare, vi segnaliamo anche l'allegato B alla presente contenente la comunicazione da trasmettere ai sensi dell'art. 33 commi 1 e 2 del GDPR "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. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione".

Riservandoci di fornire ulteriori istruzioni e comunicazioni in merito, rimaniamo a disposizione per ogni chiarimento.

Per conto del Titolare del trattamento

Il Delegato Interno Privacy

.....

ALLEGATO A

SCHEDA ANAGRAFICA DEL CANDIDATO RESPONSABILE ESTERNO DEL TRATTAMENTO

Da inviare tramite PEC

Denominazione (nome della ditta o azienda o ragione sociale)

Forma giuridica :_____

codice fiscale :_____

P. IVA :_____

sede legale in:

Comune _____ prov. |__|__| Stato _____

indirizzo _____ n. _____ C.A.P. |__|__|__|__|__|

Telefono fisso _____ cell. _____

Email _____@_____

PEC _____@_____

Sito web _____

Altro domicilio elettronico per invio delle comunicazioni inerenti _____

REFERENTI PER L'AMMINISTRAZIONE:

Cognome _____ Nome _____

codice fiscale |__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__| sesso |__|

Telefono fisso _____ cell. _____

Email _____@_____

PEC _____@_____

REFERENTI PER L'AMMINISTRAZIONE:

Cognome _____ Nome _____

codice fiscale |__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__| sesso |__|

Telefono fisso _____ cell. _____

Email _____@_____

PEC _____@_____

RESPONSABILE DELLA PROTEZIONE DATI (DPO) – SE NOMINATO:

Cognome _____ Nome _____

codice fiscale |__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__| sesso |__|

Telefono fisso _____ cell. _____

Email _____@_____

PEC _____@_____

BANCHE DATI TRATTATE PER CONTO DELL'ENTE:

_____

_____

_____

NOTE:

_____

_____

Il sottoscritto dichiara:

[ ] di aver predisposto un registro dei trattamenti effettuati per conto dell'Ente che trasmette unitamente alla presente

[ ] di NON aver predisposto un registro dei trattamenti effettuati per conto dell'Ente in quanto _____

Il sottoscritto dichiara di avere i requisiti per lo svolgimento delle attività di Responsabile del trattamento (art. 30 del GDPR) e che è a conoscenza che i trattamenti dei dati per conto del Titolare dovrà avvenire nel rispetto della vigente normativa nonchè delle modalità:

1) contenute nel contratto di affidamento del servizio (e successive variazioni)

2) negli atti di incarico/nomina specifici

3) nelle comunicazioni, verbali ed altri atti in cui sono state fornite istruzioni

4) nella manualistica a corredo e supporto delle banche dati

Il sottoscritto dichiara di essere in particolare a conoscenza che:

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento (o sub-responsabili), dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

Quando un responsabile del trattamento ricorre a un secondo responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale ulteriore responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora un secondo responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del secondo responsabile.

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare 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.

Il titolare del trattamento (eventuali Co-titolari), il responsabile del trattamento e, ove applicabile, un Rappresentante (così come definito nelle norme europee), cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire ulteriori livelli di sicurezza adeguato al rischio, 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.

Articolo 33 - Notifica di una violazione dei dati personali all'autorità di controllo

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.

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

3. La notifica di cui al paragrafo 1 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.

4. 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.

5. Il titolare del trattamento documenta 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 del presente articolo.

Luogo: _____ Data: _____

Il legale rappresentante

.....

ALLEGATO B

MODELLO PER LA COMUNICAZIONE DELLA VIOLAZIONE DEI DATI DAL RESPONSABILE AL TITOLARE (AI FINI DEL C.D. "DATA BREACH")

inviare tramite PEC

Denominazione (nome della ditta o azienda o ragione sociale)

_____

Forma giuridica _____

codice fiscale _____

P. IVA _____

sede legale in:

Comune _____ prov. |__|__| Stato _____

indirizzo _____ n. _____ C.A.P. |__|__|__|__|__|

Telefono fisso _____ cell. _____

Email _____@_____

PEC _____@_____

Sito web _____

Altro domicilio elettronico per invio

delle comunicazioni inerenti _____

REFERENTI:

Cognome _____ Nome _____

codice fiscale |__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__| sesso |__|

Telefono fisso _____ cell. _____

Email _____@_____

PEC _____@_____

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

_____

_____

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

[ ] Il _____

[ ] Tra il _____ e il _____

[ ] In un tempo non ancora determinato

[ ] E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____

_____

_____

Modalità di esposizione al rischio - Tipo di violazione

[ ] Lettura (presumibilmente i dati non sono stati copiati)

[ ] Copia (i dati sono ancora presenti sui sistemi del titolare)

[ ] Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

[ ] Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

[ ] Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

[ ] Altro :

_____

Dispositivo oggetto della violazione

[ ] Computer

[ ] Rete

[ ] Dispositivo mobile

[ ] File o parte di un file

[ ] Strumento di backup

[ ] Documento cartaceo

[ ] Altro :

_____

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____

_____

_____

_____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

[ ] N. _____ persone

[ ] Circa _____ persone

[ ] Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

[ ] Dati anagrafici/codice fiscale

[ ] Dati di accesso e di identificazione (user name, password, customer ID, altro)

[ ] Dati relativi a minori

[ ] Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale

[ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale

[ ] Dati giudiziari

[ ] Copia per immagine su supporto informatico di documenti analogici

[ ] Ancora sconosciuto

[ ] Altro :

_____

_____

_____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

[ ] Basso/trascurabile

[ ] Medio

[ ] Alto

[ ] Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

Si ritiene che la violazione vada comunicata anche agli interessati?

Sì, perchè _____

No, perchè _____

Qual è il contenuto della comunicazione da rendere agli interessati?

_____

_____

_____

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

_____

_____

_____

_____

_____

Il legale rappresentante

.....