Studio Legale
PRAGLIOLA

GeneralDataProtectionRegulation

(REG. UE 679/2016)

ALBIGNASEGO 6 GIUGNO 2018

Confagricoltura
Padova

Ho letto tutta l'informativa sulla Privacy.
Alla fine lui muore!

IL PERCORSO CHE CI HA ACCOMPAGNATO AL 25 MAGGIO 2018 DALLA DIRETTIVA MADRE 95/46 CE

N.B. Il Regolamento si applica solo ai dati delle PERSONE FISICHE

SIAMO ABITUATI A REGALE INFORMAZIONI SULLA NOSTRA PERSONA…

…MA NON SAPPIAMO QUASI MAI COME QUELLE INFORMAZIONI VENGANO RIUTILIZZATE

AMBITO DI APPLICAZIONE (sintesi)

- Relativo alla protezione delle **persone fisiche** (non decedute) con riguardo al trattamento dei dati personali (non anonimi), nonchè alla libera circolazione di tali dati.
- Dati personali della persona fisica **(INTERESSATO)** che si trovi nell'Unione Europea, indipendentemente dalla nazionalità.
- **Si applica** al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi (srt. 2 paragrafo 1)

Non si applica ai trattamenti effettuati

- Da una persona fisica per attività di carattere esclusivamente personale e domestico;
- Dalle Autorità per prevenzione o perseguimento di reati o esecuzioni di sanzioni penali;
- Dagli Stati membri nell'esercizio di attività relative alla politica esterna e di sicurezza comune.

CONTENUTO DEL DGPR

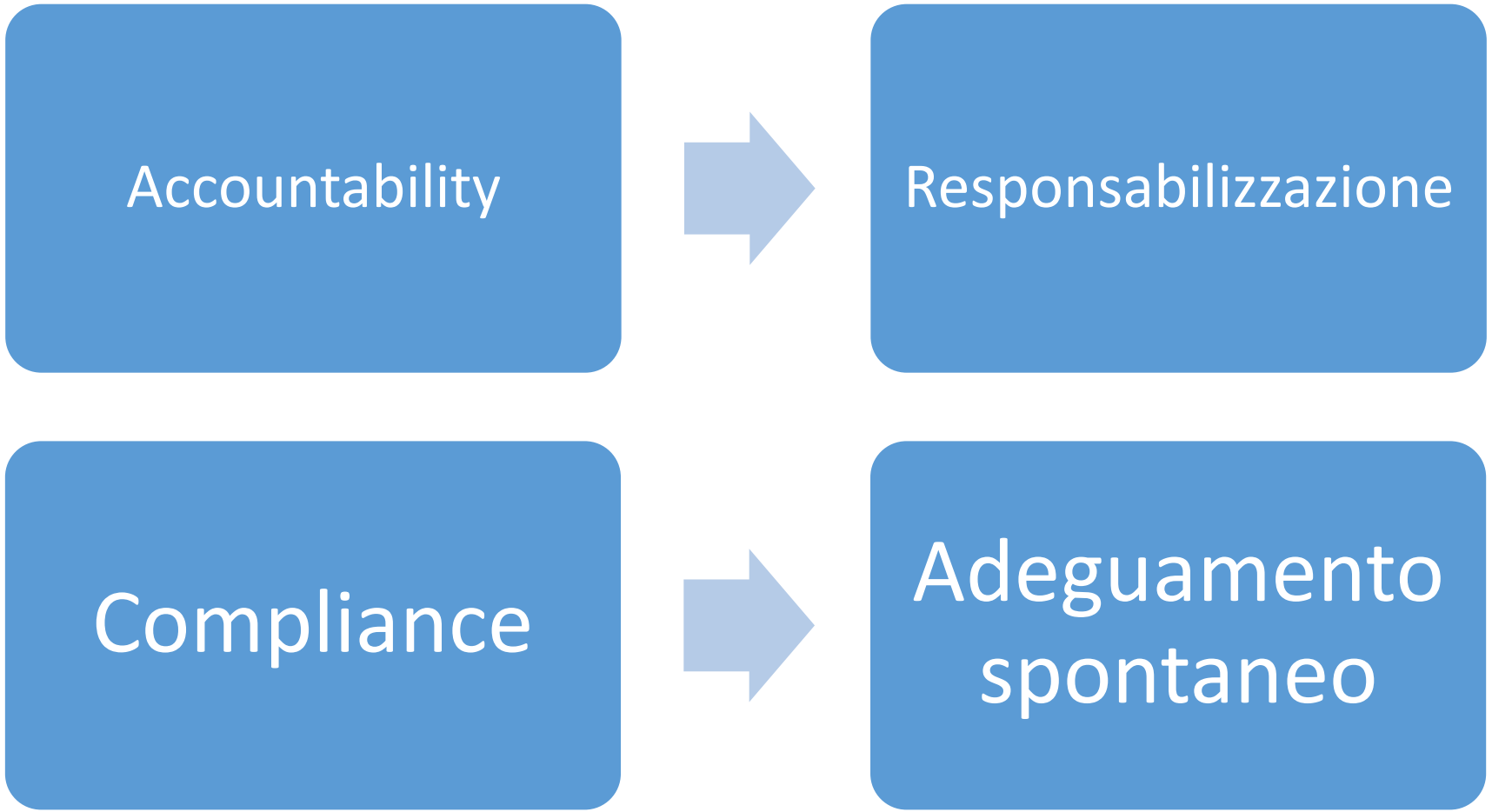
- **CONFERMA** i principi generali di: TRASPARENZA, LICEITA', PROPORZIONALITA', CONSERVAZIONE E SICUREZZA NEL TRATTAMENTO DEI DATI.
- **MODIFICA** norme e adempimenti precedenti:
- - informativa da rendere all'interessato;
- - CONSENSO dell'interessato;
- - ripartizione delle responsabilità;
- - diritto di accesso, di rettifica e di oppozione dell'interessato;
- - sanzioni.

CONTENUTO DEL DGPR

INTRODUCE norme e adempimenti DEL TUTTO NUOVI:

- Sicurezza del trattamento;
- Responsabilizzazione (accountability);
- Registro dei trattamenti;
- Valutazione di impatto;
- Violazione dei dati (data Breach);
- D.P.O. – Data Protection officer;
- Privacy by design e privacy by defoult (protezione della progettazione e protezione per impostazione predefinita);
- Diritto obblio;
- Diritto alla limitazione del trattamento;
- Diritto alla portabilità dei dati.

Concetti chiave che vengono introdotti con il GDPR



ACCOUNTABILITY

Responsabilizzazione e obbligo generale di prova degli adempimenti (art. 24)

All’esito dell’attività di conformazione al Regolamento, il Titolare deve:

1- Essere in grado di dimostrare che i trattamenti avvengono in conformità al regolamento, mediante un REGISTRO DEI TRATTAMENTI da mettere a disposizione del Garante per i controlli;

2- Aggiornare sia le misure che il documento qualora necessario (ad es. In caso di introduzione di nuovi tipi di trattamenti, di aggiunta o venir meno di tipologie di dati trattati, di modifiche delle normative di settore);

3 - Introdurre policy in materia di protezione dati, e applicarle/pubblicarle (formare il personale!);

4 - Designare un DPO (in alcuni casi obbligatorio, in altri altamente consigliato) e comunicare il nominativo all’Autorità Garante;

ACCOUNTABILITY

Responsabilizzazione e obbligo generale di prova degli adempimenti (art. 24)

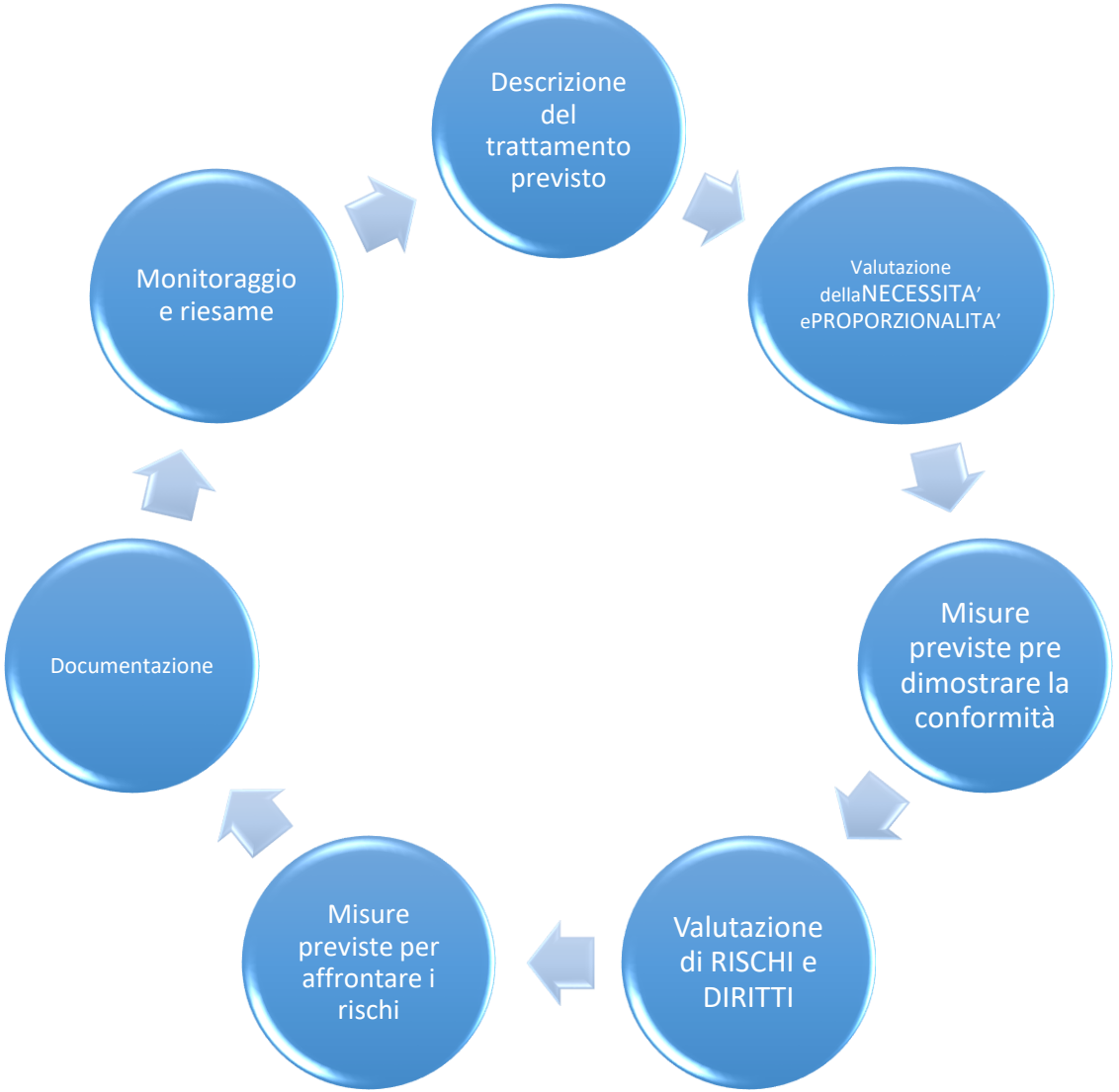
5 - Creare le procedure di gestione dei diritti degli Interessati (stabilendo regole per l'accesso, la gestione del contenzioso, il riscontro tempestivo etc.);

6 - Introdurre le procedure per la rilevazione e comunicazione (se del caso) dei «data breach»;

7 - Effettuare la valutazione dei rischi relativi ad ogni singolo trattamento (ivi inclusa la valutazione dell'adeguatezza delle misure tecnologiche/fisiche adottate a protezione dei dati trattati) e redigere una DPIA;

8 - Mantenere costantemente aggiornato e verificato il sistema «privacy/data protection» introdotto.

INPUT PER REGISTRO DEI TRATTAMENTI



DEFINIZIONI (ART. 4 GDPR)

1) «**dato personale**»: 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; (C26, C27, C30)

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (C67)

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (C24, C30, C71-C72)

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (**C15**)

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (**C74**)

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (**C31**)

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)

12) «**violazione dei dati personali**»: la 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; (C85)

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (C34)

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (C51)

15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (C35).

L’INFORMATIVA

Prima di effettuare il Trattamento (quindi prima di «raccogliere» il dato) deve essere fornita all’Interessato un’INFORMATIVA ***CONCISA, TRASPARENTE, COMPRENSIBILE E FACILMENTE ACCESSIBILE***.

In essa vanno sempre indicati:

1. I dati e i contatti del Titolare del Trattamento e del DPO (ove nominato)
2. La Base Giuridica del Trattamento
3. L’eventuale TRASFERIMENTO del dato in paesi terzi
4. Il Periodo di conservazione dei dati
5. Le modalità di presentazione reclamo

IL CONSENSO

- NECESSARIO per trattare i dati personali in modo lecito;
- Non è valido se non è preceduto da un'informativa sul trattamento dei dati personali;
- Deve essere **libero, consapevole, specifico, informato, inequivocabile** e basato su un'azione positiva dell'interessato;
- NON è AMMESSO il consenso TACITO O PRESUNTO;
- Valido se è compiuto da soggetti con età maggiore di anni 16;
- DEVE essere FACILMENTE REVOCABILE.

NUOVE FINALITA’

Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all’interessato informazioni in merito a tale diversa finalità.

TITOLARE, RESPONSABILE E D.P.O.DEL TRATTAMENTO (ART. 24 GDPR)

TITOLARE DEL TRATTAMENTO

È il soggetto (persona fisica, giuridica o ente) che determina le finalità e i mezzi del trattamento dei dati. Se il Titolare non è stabilito (ovvero non risiede o non ha sede legale nell'U.E.), deve avere un rappresentante nell'Unione Europea.

RESPONSABILE DEL TRATTAMENTO

È il soggetto che tratta dati personali per conto del Titolare. Necessaria una nomina formale che contenga al suo interno specifici obblighi e doveri sullo stesso incombenti.

D.P.O. (DATA PROTECTION OFFICER)

Obbligo di nomina da parte di:

- Enti pubblici;
- Privati la cui attività principale richiede trattamenti con monitoraggio regolare e sistematico degli interessati su larga scala;
- Privati la cui attività principale richiede il trattamento su larga scala di dati particolari o penali.

PRIVACY BY DESIGN E BY DEFAULT

PRIVACY BY DESIGN (PROTEZIONE DEI DATI SIN DALLA PROGETTAZIONE)

Risk assessment in fase di progettazione e sviluppo di prodotti / servizi/ applicazioni

PRIVACY BY DEFAULT (PROTEZIONE DEI DATI PER IMPOSTAZIONE PREDEFINITA)

- Adottare misure tecniche e organizzative e procedure adeguate a garantire un trattamento conforme al GDPR;
- Adottare meccanismi predefiniti per garantire che siano trattati solo i dati necessari per ciascuna finalità (minimizzazione, pseudonimizzazione), che non siano accessibili ad un numero indeterminato di persona e siano conservati non oltre il tempo necessario.

SICUREZZA DEL TRATTAMENTO

VALUTAZIONE PRELIMINARE de:

- La natura, l'oggetto, il contesto e le finalità del trattamento;
- Il rischio e la gravità per i diritti e le libertà delle persone fisiche.

ADEGUAMENTO DELLE MISURE DI SICUREZZA AL RISCHIO RILEVATO MEDIANTE:

- Misure tecniche e organizzative ad hoc;
- Pseudonomizzazione dei dati personali;
- Misure che garantiscono la riservatezza, l'integrità, la disponibilità, e la resilienza dei sistemi e dei servizi di trattamento dei dato;
- Capacità di ripristino tempestivo della disponibilità dei dati in caso di incidente fisico o tencio;
- Procedura per testare regolamente l'efficacia delle misure tecniche e organizzative.

PSEUDONIMIZZAZIONE

Processo in base al quale i dati sono conservati in un formato che impedisce di identificare direttamente un individuo senza l'utilizzo di informazioni aggiuntive.

Tecniche di «data masking»:

- Usare valori random per sesso e razza;
- Usare valori casuali per le date di nascita;
- Generare numeri causali per inumeri civici;
- Utilizzare un generatore di e-mail;
- Utilizzare un generatore di nomi di società.

VIOLAZIONE DEI DATI (DATA BREACH)

Obbligo di notifica al Garante degli eventi che comportano perdita, distruzione o diffusione indebita di dati.

No: se i dati personali coinvolti nella violazione sono già disponibili pubblicamente

Sì: alla notifica in caso di violazioni che coinvolgono dati trattati non disponibili pubblicamente relativi a clienti, dipendenti, fornitori.

- Se il rischio per i diritti e le libertà degli interessati è probabile, deve notificare la violazione al Garante, ove possibile entro 72 ore e, comunque, senza giustificato ritardo;
- Comunicare agli interessati la violazione in caso di rischio elevato oppure su richiesta del Garante

IL GARANTE

Il Garante per la protezione dei dati personali:

- Svolge indagini sull'applicazione della normativa;
- Esamina i reclami degli interessati;
- Infligge sanzioni amministrative;
- Rilascia autorizzazioni preliminari;
- Approva i Codici di condotta;
- Rilascia certificazioni;
- Promuove la comprensione della materia
- Ha poteri: di indagine, correttivi, autorizzativi e consuntivi

SANZIONI AMMINISTRATIVE

Il Garante della Privacy, a seguito di indagini proprie (svolte tramite ispettori interni o tramite la Guardia di Finanza) o di reclami formulati da soggetti pubblici o privati

EMANA:

- AVVERTIMENTI
- AMMONIMENTI
- INGIUNZIONI
- INIBIZIONI AL TRATTAMENTO
- SANZIONI PECUNIARIE

OPPOSIZIONE:

E’ ammesso il ricorso all’Autorità Giudiziaria Ordinaria contro la decisione sul Garante

SANZIONI AMMINISTRATIVE PECUNIARIE

VALORE

- Fino a 20 Milioni di Euro
- Oppure, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente

IN QUALI CASI:

- Violazioni del regolamento;
- Inosservanzza di un ordine impartito dal Garante della Privacy Nazionale.

CRITERI DI GRADAZIONE DELLA SANZIONE

- Natura, gravità e durata dell'illecito;
- Carattere internazionale doloso o colposo dell'illecito;
- Recidività;
- Altre aggravanti/attenuanti

RISARCIMENTO DEL DANNO

CHI PUO' CHIEDERLO:

Chiunque abbia subito un danno: interessato o terzo

COSA PUO' CHIEDERE:

Danni patrimoniali e non patrimoniali

A CHI RIVOLGERSI:

Autorità Giudiziaria Ordinaria

CONTRO CHI:

Titolare o Responsabile. In caso di Contitolari questi rispondono in solido.

ESONERO DA RESPONSABILITA':

Evento dannoso non imputabile

RIASSUNTO DEGLI ADEMPIMENTI MINIMI

Confagricoltura Padova — Studio Legale PRAGLIOLA

ADEMPIMENTI OPERATIVI AL GDPR

Dall'attenzione alla privacy, alla protezione del dato

	Obbligo	Facoltativo / Obbligatorio solo per determinate realta'	Consigliato
Redigere MODULISTICA chiara, sintetica ed esaustiva *(INFORMATIVA + CONSENSO AL TRATTAMENTO)*	✓		
Strutturare un idoneo REGISTRO DEI TRATTAMENTI (uno strumento dove appuntiamo tutte le attivit à di trattamento dei dati personali)		✓	✓
Effettuare un'analisi della filiera del dato all'interno dell'azienda ed effettuare una idonea mappatura del rischio attraverso una DPIA		✓	

Valutazioni minime da effettuare all'interno dell'azienda

ACQUISIZIONE DEL CONSENSO

- Ho predisposto una modulistica idonea per informare e raccogliere il consenso degli interessati (dipendenti/fornitori/clienti)?
- Ho stabilito delle privacy policy idonee al trattamento dei dati interno alla mia azienda?
- Ho aggiornato il mio sito internet con idonee check-box o campi predisposti a raccogliere il consenso?

CONSERVAZIONE DEL DATO

- Sui device aziendali (computer, tablet, smartphone, server, NAS,...) effettuiamo backup, siamo dotati di antivirus e firewall, abbiamo predisposto l'utilizzo e l'aggiornamento di password, è partizionato l'accesso alle cartelle?
- I documenti cartecei, sono custoditi in modo idoneo a garantirne l'anonimato, la sicurezza e l'integrità?
- I documenti sono conservati in cassetto/armadio/archivio non accessibile a persone non autorizzate o chiusi a chiave?
- Ho stabilito mezzi e procedure per adempiere ai nuovi diritti stabiliti dal GDPR a favore del consumatore? (comunicazione dei dati in nostro possesso, portabilità, minimizzazione,...)

CANCELLAZIONE DEL DATO

- Ho stabilito (e comunicato nell'informativa/privacy policy) le tempistiche e le modalità prestabilite per la cancellazione del dato ?
- Ho stabilito dei sistemi di verifica sull'effettiva cancellazione del dato dai sistemi di archiviazione aziendale?

IN CASO DI DATA BREACH

- Ho stabilito le modalità per darne TEMPESTIVA comunicazione agli utenti interessati?
- Ho stabilito le modalità per darne TEMPESTIVA (72 ore dalla scoperta) comunicazione alle autorità di controllo?

LA SINTESI DEL GDPR

«Grazie della pazienza e buon lavoro a tutti»