RIZZATO-DAINESE

ECONOMIA DIRITTO FINANZA LAVORO

GLI PSICOLOGI E LA PRIVACY

adeguamento al GDPR
Regolamento UE 2016/679

NORMATIVA E TEMPISTICA

- D.Lgs 196/2003 ancora vigente
- Regolamento UE 679/2016 in vigore dal 25 maggio 2018 (=GDPR)

- Legge delega 163/2017 – art. 13 per l'approvazione di un decreto di adeguamento
- Schema di decreto tuttora in bozza

NORMATIVA E TEMPISTICA

Ciò premesso:

- 25 maggio: punto di partenza, non di arrivo
- non ci sono ragioni per procrastinare le iniziative almeno laddove il quadro è già definito

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

IL PERCORSO CHE CONDUCE ALL'ADEGUAMENTO

- Mappatura dei dati e dei trattamenti
- Individuazione dei rischi che incombono sui dati ed eventuale predisposizione della valutazione d'impatto - DPIA
- Mappatura dei soggetti da autorizzare (incaricati) o ai quali conferire nomine specifiche di natura contrattuale (responsabili)
- Iniziative connesse all'informativa, al consenso, all'esercizio dei diritti da parte dell'interessato
- Individuazione delle misure sufficienti a garantire la sicurezza e la riservatezza dei dati

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

IL PERCORSO CHE CONDUCE ALL'ADEGUAMENTO

- Programmazione sistematica di verifiche periodiche dell'efficacia delle misure adottate, in modo da garantirne l'adeguatezza nel tempo anche in ragione delle mutate tecnologie o dei mutati tipi di trattamento o di finalità
- Formazione degli operatori e programmazione di un'attività di vigilanza costante ed eventuale nomina del DPO

- La realizzazione di tale percorso va comprovata dalla rendicontazione sistematica e standardizzata di tutte le attività svolte

  => Registro dei trattamenti

MAPPATURA DEI DATI

Sono dati personali, tra gli altri,

- i dati identificativi
- i dati sensibili (=dati particolari per il GDPR)
- i dati anonimi (in quanto tali non soggetti a tutela)

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

Pseudonimizzazione

- Si tratta di un’operazione di trattamento atta a fare in modo 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 adeguate allo scopo

MAPPATURA DEI DATI

Sono soggetti a tutela

- i dati delle sole persone fisiche

- oggetto di trattamenti automatizzati

oppure

- contenuti in un archivio

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

TRATTAMENTO DEI DATI

Definizione di trattamento

- Il trattamento è qualsiasi operazione, svolta manualmente o in modo automatizzato, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

TRATTAMENTO DEI DATI

Principi base del trattamento

- Liceità, correttezza, trasparenza
- Finalità determinate ed esplicite
- Minimizzazione dei dati (pertinenti rispetto alle finalità)
- Esattezza e aggiornamento
- Limitazione nel tempo (non oltre il conseguimento delle finalità)
- Integrità e riservatezza

TRATTAMENTO DEI DATI

Base giuridica del trattamento

- esecuzione di un contratto
- adempimento di un obbligo di legge
- consenso dell'interessato

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Interessato

- La persona fisica identificata o identificabile anche in via indiretta

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Titolare

- la persona fisica o giuridica che determina, singolarmente o insieme ad altri, le finalità e i mezzi del trattamento di dati personali (secondo il nuovo principio dell'accountability)

=> quindi chi ha potere decisionale

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Contitolare

- Se due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno il cui contenuto essenziale è messo a disposizione dell'interessato, le rispettive responsabilità ai fini privacy che dovranno essere coerenti con i rispettivi ruoli e rapporti con l'interessato

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Esistono soggetti diversi dal titolare che effettuano trattamento di dati?

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Responsabile

- la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
- la nomina ha natura contrattuale (quindi implica accettazione) e contenuto definito (art. 28 GDPR)
- il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento

SOGGETTI DEL TRATTAMENTO

Responsabile - quali obblighi?

- Segue le istruzioni impartitegli (per iscritto) dal titolare pur nell'ambito di una certa autonomia
- Rispetta gli obblighi fissati dal GDPR per la sua figura

=> Ha una responsabilità contrattuale nei confronti del titolare e una responsabilità diretta (conferitagli dalla normativa comunitaria) nei confronti dell'interessato

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Responsabile - esempi

- libero professionista collaboratore di struttura complessa
- (quindi lo psicologo può essere a sua volta responsabile per conto di un titolare terzo)

- commercialista
- servizi di cloud computing
- fornitori genericamente intesi =>verificarne l'affidabilità nel trattamento dei dati personali

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

Incaricato

- Gli incaricati sono i soggetti (necessariamente persone fisiche) autorizzati dal titolare o dal responsabile a compiere specifiche operazioni di trattamento dei dati, sotto l'autorità del titolare e/o del responsabile
- La legge impone al titolare di verificare ed aggiornare annualmente l'ambito di trattamento dei soggetti incaricati

SOGGETTI DEL TRATTAMENTO

Incaricato - esempi

- segretaria/dipendente

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

SOGGETTI DEL TRATTAMENTO

Formazione

- Vanno istituiti momenti di formazione e informazione di vario livello destinati a tutti gli operatori
- Vanno definiti codici di condotta e procedure
- L'obbligo di formazione degli incaricati e di vigilanza sull'operato degli stessi è condiviso da titolare e responsabile ed incide in maniera significativa sulla portata della loro responsabilità sotto il profilo sanzionatorio

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

DPO (o RDP) – nuova figura

- Si tratta di un organo indipendente di vigilanza del sistema di conformità al GDPR
- La nomina di tale figura è obbligatoria per le PA, nonché in presenza di circostanze di maggior rischio. Il ruolo può essere rivestito sia da persone interne che esterne, purché siano garantite competenza specifica e indipendenza di giudizio

DPO (o RDP) – nuova figura

- Dalle FAQ diffuse dal Garante Privacy emerge il chiaro pensiero che le società operanti nel settore della cura della salute, della prevenzione e della diagnosi sanitaria siano tenute alla nomina del DPO
- La necessità di procedere a tale nomina pare invece meno sentita negli studi mono-professionali, pur restando però necessaria una valutazione specifica che tenga conto di volta in volta del caso concreto

DPO (o RDP) – nuova figura

- Anche ove il Regolamento non imponga la designazione di un DPO, la sua nomina su base volontaria è comunque incoraggiata
- Se nominato il DPO deve rispettare i requisiti previsti dagli art. 37 e 39 del Regolamento
- Della sua nomina va data comunicazione al Garante mediante apposita procedura informatica

DPO (o RDP) – requisiti

- È designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e della capacità di assolvere i compiti di cui all'art.39
- La nomina deve garantire indipendenza e assenza di conflitto di interessi, in particolare il DPO non può quindi rivestire un ruolo che comporti la definizione delle finalità o delle modalità di trattamento (che spettano invece al titolare e al responsabile)

DPO (o RDP) - compiti

- Informa e fornisce consulenza al titolare e/o al responsabile, nonché agli incaricati in merito agli obblighi derivanti dal Regolamento
- Vigila sull'osservanza del Regolamento
- Formula pareri, in particolare nello svolgimento della valutazione d'impatto sulla protezione dei dati (cosiddetta DPIA)
- Coopera durante l'attività di controllo, è punto di contatto e facilitatore in caso di violazioni o di esercizio dei propri diritti da parte degli interessati al trattamento

INFORMATIVA, CONSENSO E DIRITTI DELL'INTERESSATO

Informativa

- contenuto tassativo
- linguaggio chiaro e semplice
- finalità determinate

- atteso che l'informativa si arricchisce di nuovi contenuti per effetto dell'entrata in vigore del GDPR, il titolare del trattamento, è tenuto ad adeguarne il contenuto non solo con riferimento ai nuovi trattamenti, ma anche con riferimento a quelli in corso

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

Informativa - contenuto

- Indicazione del titolare, ed eventualmente del DPO, con i relativi dati di contatto
- Finalità e base giuridica del trattamento
- Conseguenze del mancato consenso
- Destinatari dei dati o categorie di destinatari
- L'eventuale trasferimento di dati in paesi terzi (attenzione ai server in remoto)
- Periodo di conservazione o criteri per stabilirlo
- Esplicitazione dei diritti dell'interessato

Informativa - tempistica

- All'atto della comunicazione dei dati => subito

- Entro 1 mese dalla comunicazione se i dati non sono raccolti direttamente dall'interessato, ma presso terzi

- Ok anche se in formato elettronico (mail o sito web)

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

INFORMATIVA, CONSENSO E DIRITTI DELL'INTERESSATO

Consenso

- libero, specifico, informato, inequivocabile
- **esplicito** per i dati sensibili

- richiesta chiaramente distinguibile (se inserito in un documento complesso)
- no a caselle pre-spuntate

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

INFORMATIVA, CONSENSO E DIRITTI DELL'INTERESSATO

Vecchi (ma confermati) diritti dell'interessato

- diritto all'informativa
- diritto di accesso ai dati
- diritto di chiederne la rettifica
- diritto di cancellazione (oggi rafforzato: diritto all'oblio)
- diritto di opposizione

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

Nuovi diritti dell'interessato

- diritto di limitazione del trattamento (raccolta di dati non eccedenti lo scopo e per periodi di tempo definiti)
- diritto alla portabilità dei dati (=possibilità per gli interessati di ottenere copie dei propri dati personali per poterle trasmettere ad altri titolari, anche direttamente)

- risposta entro 1 mese (estensibili a 3 in caso di particolare complessità)

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

MISURE DI SICUREZZA

Accountability (o responsabilizzazione)

- nuovo principio ispiratore del GDPR
- dalle misure minime … alle misure sufficienti

=> adozione di modelli organizzativi e misure idonee a garantire la riservatezza dei dati trattati e la conformità del trattamento alle previsioni regolamentari, soprattutto con riferimento alle procedure di sicurezza informatica

Accountability (o responsabilizzazione)

- Prima di procedere al trattamento bisogna prevedere le garanzie (=misure di sicurezza sufficienti) indispensabili per tutelare i diritti degli interessati
- Tale attività deve essere specifica e dimostrabile
- La rete documentale ha quindi rilevanza probatoria

Accountability (o responsabilizzazione)

- La responsabilizzazione impone di monitorare costantemente nel tempo le eventuali modifiche alle operazioni di trattamento che possano richiedere l'adozione di procedure diverse (si pensi ad esempio al caso in cui lo sfruttamento dei dati personali avviene per finalità diverse da quelle originarie, oppure all'introduzione di nuove tecnologie informatiche)

MISURE DI SICUREZZA

Censimento dei dati trattati e dei processi di trattamento

- si tratta dell'attività prodromica, volta a verificare l'esigenza di procedere o meno con la

Valutazione d'impatto (DPIA)

- invero obbligatoria solo se il trattamento per sua natura presenta rischi specifici per diritti e libertà degli interessati come, ad esempio, per il trattamento di dati sensibili su larga scala

MISURE DI SICUREZZA

Data breach (=violazione dei dati)

- Si tratta della:
- perdita, distruzione, diffusione, manomissione, accesso non autorizzato ai dati per causa accidentale o illecita

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

MISURE DI SICUREZZA

Data breach (=violazione dei dati)

Notifica obbligatoria se è probabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche

- al Garante entro 72 ore (e comunque senza ingiustificato ritardo)
- all'interessato (solo se il rischio di cui sopra è elevato)

Via Altinate, 72
35121 Padova
T. 049 876 4168
F. 049 877 6323
info@rizzatodainese.it
www.rizzatodainese.it

Registro del trattamento

- istituzione quasi sempre opportuna, al di là dell'obbligo
- caldeggiata dal Garante
- prova del rispetto del principio di «accountability»
- anche in formato elettronico
- soggetto a periodico aggiornamento
- forma libera

Registro del trattamento - contenuto

- nome e dati di contatto dei soggetti del trattamento
- finalità del trattamento
- categorie di interessati e di dati personali
- categorie di destinatari a cui i dati personali sono comunicati, ivi compresi eventuali trasferimenti di dati in un paese terzo
- termini per la cancellazione delle diverse categorie di dati
- descrizione generale delle misure di sicurezza tecniche e organizzative adottate

SANZIONI

Tipologia delle sanzioni

- Tutela amministrativa => pesanti sanzioni pecuniarie
- Tutela giurisdizionale => azione per il risarcimento del danno patrimoniale o morale
- Tutela giurisdizionale => procedimento penale in caso di fattispecie di reato

Soggetti responsabili

- Titolare > per violazione del GDPR
- Responsabile > per violazione del GDPR o delle istruzioni impartitegli dal titolare
- Incaricati > solo in caso di grave negligenza, imprudenza, imperizia, nonché di violazione del segreto professionale

RIZZATO–DAINESE
ECONOMIA DIRITTO FINANZA LAVORO

Via Altinate, 72
35121 Padova

T. 049 876 4168
F. 049 877 6323

info@rizzatodainese.it
www.rizzatodainese.it