UNO QUATTRO
STUDIO LEGALE

Compliance al Regolamento Generale sulla Protezione dei Dati Personali (GDPR): Principi della Riforma, nuovi adempimenti e prime riflessioni sulle implicazioni nel settore Toys & Kids

- Convegno ASSOGIOCATTOLI del 28/02/2018 -

DI CHE COSA PARLEREMO OGGI

Parte Prima – Avv. Corrado Blandini

1) A cosa serve il GDPR

2) Alcuni concetti chiave:
   - «dati personali»
   - cosa si intende per «trattamento»
   - chi sono i protagonisti principali del GDPR
   - a chi si applica il GDPR

3) Principi della Riforma

4) Alcune delle principali novità

PARTE PRIMA

- A COSA SERVE IL GDPR -

"Ogni persona ha **diritto alla protezione dei dati di carattere personale** che la riguardano"

(Cfr. Art. 8 Carta dei Diritti Fondamentali dell'Unione Europea)

Diffusione Globale dei Dati + Trattamenti più sofisticati

= Rischi più elevati

Il GDPR si propone di **rafforzare la tutela** del diritto alla protezione dei dati e **regolare la libera circolazione** dei dati nell'UE

ALTRI OBIETTIVI DEL GDPR

1) Equiparare il livello di protezione in tutti gli Stati UE
   → Diritti degli Interessati & Obblighi di Titolari / Responsabili

2) Assicurare una applicazione coerente e omogenea delle norme in tutti gli Stati UE
   → Poteri & Cooperazione tra Authorities

3) Fornire alle aziende europee maggiore competitività (valorizzazione economica dei dati, big data, recupero della fiducia del consumatore, etc…)

- ALCUNI CONCETTI CHIAVE -

DATI PERSONALI

Qualsiasi informazione riguardante una persona **fisica** identificata o identificabile

Si considera «**identificabile**» la persona fisica che, direttamente o indirettamente, può essere **messa in relazione** ad un elemento che ne consente l'**individuazione** (es. nome, ubicazione ovvero altri elementi della sua identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale, etc…)

- ALCUNI CONCETTI CHIAVE -

CATEGORIE PARTICOLARI DI DATI PERSONALI

Sono i dati personali che rivelano:
- origine razziale o etnica
- credo politico, religioso o filosofico
- appartenenza sindacale

A questa categoria appartengono anche:
- Dati genetici
- Dati biometrici
- Dati relativi alla salute
- Dati relativi alla vita sessuale o all'orientamento sessuale

Il trattamento di tali dati è, di regola, **VIETATO**, salvo che ricorrano casi particolari espressamente disciplinati

- ALCUNI CONCETTI CHIAVE -

COSA SI INTENDE PER «TRATTAMENTO» ?

Qualsiasi **operazione, manuale o automatizzata, applicata** a dati personali.

Alcuni Esempi :

- Raccolta
- Registrazione
- Organizzazione
- Conservazione
- Comunicazione

NOTA L'elenco esaustivo è contenuto all'art. 2 GDPR, alla voce «Trattamento», e include: Raccolta, Registrazione, Organizzazione, Strutturazione, Conservazione , Adattamento, Modifica, Estrazione, Consultazione, Uso, Comunicazione mediante trasmissione, Diffusione, Altra forma di messa a disposizione, Raffronto o interconnessione, Limitazione, cancellazione o distruzione

- ALCUNI CONCETTI CHIAVE -

Chi sono i protagonisti principali del GDPR ?

Interessato: la persona fisica i cui dati personali vengono trattati

Titolare del trattamento: il soggetto (persona fisica, giuridica, autorità o ente) che determina le finalità e i mezzi del trattamento

Responsabile del trattamento: il soggetto (persona fisica, giuridica, autorità o ente) che tratta dati personali per conto del Titolare in forza di un contratto

Responsabile della protezione dei dati (DPO) : il dipendente o il consulente, designato dal Titolare o dal Responsabile nei casi di cui all'art. 37 GDPR, responsabile dei compiti indicati dall'art. 39 GDPR

- ALCUNI CONCETTI CHIAVE -

A chi si applica il GDPR ?

1) A coloro che, essendo **stabiliti** nell'UE o in luogo soggetto al diritto di uno Stato Membro, effettuano trattamenti di dati personali

2) A coloro che, pur **NON** essendo **stabiliti** nell'UE, effettuano trattamenti di dati personali di interessati che si trovano nell'UE, quando tali attività di trattamento riguardano:

   a) l'offerta di beni e servizi ai suddetti interessati, anche a titolo gratuito;

   b) il monitoraggio dei loro comportamenti quando hanno luogo all'interno dell'UE

- PRINCIPI DELLA RIFORMA -

1) PRINCIPI DEL TRATTAMENTO DEI DATI

a) Liceità, Correttezza e Trasparenza nei confronti dell'Interessato

- il trattamento deve avvenire in forza di una valida **base giuridica** (es. consenso, adempimento di obblighi contrattuali o di legge, etc..)

- l'interessato deve essere informato della **esistenza** e delle **finalità** del trattamento al **momento della raccolta** del dato → l'informazione deve essere *facilmente accessibile* e *comprensibile*, dunque messa in evidenza e formulata in un linguaggio chiaro e semplice

- il Titolare deve essere trasparente anche in merito alle **modalità** con cui i dati vengano raccolti e alla **misura** in cui vengono trattati

- PRINCIPI DELLA RIFORMA -

b) Limitazione della finalità

Si possono **raccogliere** dati solo per finalità determinate, esplicite e legittime

Li si può **successivamente trattare** solo per ulteriori finalità che non siano incompatibili con quelle iniziali (es. precontrattuali e contrattuali)

c) Minimizzazione dei dati

I dati personali sono adeguati, pertinenti e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati

d) Esattezza dei dati

I dati devono essere esatti e, se necessario rispetto alle finalità per le quali sono trattati, mantenuti aggiornati cancellando o rettificando quelli inesatti

- PRINCIPI DELLA RIFORMA -

e) Limitazione della conservazione

I dati personali vanno conservati solo per il tempo strettamente necessario al conseguimento della finalità per la quale furono raccolti

f) Integrità e riservatezza

I dati vanno trattati in maniera tale da garantirne un'adeguata sicurezza, compresa la **protezione** – mediante misure tecniche ed organizzative adeguate (es. cifratura, pseudonimizzazione, anonimizzazione, etc…) – da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o danno accidentale dei dati

- PRINCIPI DELLA RIFORMA -

2) PRINCIPIO DI RESPONSABILIZZAZIONE (c.d. «Accountability»)

Il Titolare del trattamento ha la responsabilità di garantire che il trattamento avvenga nel rispetto dei principi del GDPR, e l'onere di dimostrarlo.

Dovrà adottare attuare **misure tecniche e organizzative adeguate** rispetto ai rischi posti dal trattamento **(proporzionalità)** ed essere in grado di documentarne **l'efficacia**

- PRINCIPI DELLA RIFORMA -

Alcuni esempi delle attività che il Titolare dovrebbe svolgere ed essere in grado di documentare per dimostrare la conformità al GDPR :

- Adozione di politiche interne e attuazione di misure che soddisfino i principi della «**privacy by design**» e «**privacy by default**» (es. riduzione al minimo del trattamento, pseudonimizzazione appena possibile, etc..)

- Scelta di responsabili che offrano garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse

- Documentazione di tutte le attività di trattamento (es. **registro**)

- Designazione di un **DPO**

- Revisione periodica dei rischi del trattamento e delle misure attuate

- ALCUNE DELLE PRINCIPALI NOVITA' -

Armonizzazione

→ riduzione dei problemi posti dalla diversa applicazione della normativa nei vari Stati Membri

Trasferimenti Extra UE

→ Il dato può essere trasferito extra UE solo verso Stati ed organizzazioni che garantiscono il medesimo livello di protezione del GDPR

Obblighi dei Responsabili

→ Nuovi requisiti e incarico scritto; specifici compiti in merito alla sicurezza dei dati e obbligo di collaborazione con il Titolare nel dimostrare compliance

Necessità

→ Devono essere raccolti, conservati e trattati solo i dati strettamente necessari a conseguire la finalità ricercata

Controllo

→ Rafforzamento diritti degli interessati (diritto alla portabilità dei dati, all'oblio e di opposizione al trattamento)

Sanzioni

→ Potenziamento dei poteri (consultivi, di investigazione e correttivi) delle Autorità Nazionali e introdotte sanzioni elevate

Data Breach

→ La notifica e la comunicazione, in caso di data breach, diventano obbligatori

Consenso

→ Libero, specifico, informato e inequivocabilmente espresso con un'azione positiva

→ Requisiti rafforzati per soggetti vulnerabili (es. minori)

DI CHE COSA PARLEREMO OGGI

Parte Seconda – Avv. Umberto Locatelli

1) GDPR e nuovo approccio alla materia

2) Come rispettare il GDPR: consigli sul metodo
   - 1° step: censimento dei trattamenti
   - 2° step: analisi dei rischi ed eventuale valutazione di impatto
   - 3° step: scelta delle misure per attenuare i rischi
   - 4° step: attuazione di misure tecniche ed organizzative adeguate

3) Focus sul settore Toys & Kids

PARTE SECONDA

- GDPR e nuovo approccio alla materia -

ADEMPIMENTI → **PROCESSO AZIENDALE**

1) Approccio basato sul rischio: *principio di responsabilizzazione*

2) Adozione di un *sistema di governance* interno, ovvero un sistema di controllo dei dati che permetta in ogni momento di documentare le decisioni assunte.

- COME RISPETTARE IL GDPR: CONSIGLI SUL METODO -

Da dove si comincia? Bisogna porsi della domande…

… INTERNAMENTE

1) Sono state censite le tipologie di dati personali trattati dall'azienda, incluse le relative finalità e modalità di trattamento e conservazione dei dati?
2) Quali misure di sicurezza sono state adottate per garantire la protezione dei dati trattati?
3) I trattamenti sono strutturati per garantire i diritti degli interessati (es. diritto di cancellazione e portabilità dei dati personali)?
4) Etc…

… E PER RISPONDERE ALL'AUTORITA'

1) Puoi fornire una mappatura delle attività di trattamento dei dati personali effettuate?
2) Puoi dimostrare che le misure di sicurezza adottate siano in grado di garantire un livello di protezione adeguato al rischio?
3) Sono rispettate le modalità e le tempistiche di risposta alle richieste avanzate dagli interessati?
4) Sono attuati piani di formazione per i dipendenti?
5) Etc.…

1° STEP: CENSIMENTO DEI TRATTAMENTI

Tipologie dei dati trattati (es. anagrafiche clienti o dipendenti, etc…)

Finalità del trattamento (es. contrattuali, marketing, profilazione, etc...)

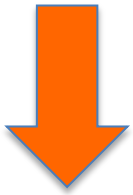
Modalità del trattamento (es. cartacea, digitale, etc…)

Categorie di soggetti interni che trattano i dati (es. HR, marketing, etc...)

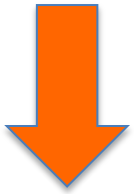
Tempi di conservazione dei dati trattati (es. richiesti dalla legge o dalla finalità del trattamento, etc…)

Eventuale trasferimento o comunicazione dei dati a terzi (es. partner commerciali, Autorità, consulenti, etc...)

Censimento dei trattamenti



Mappatura e classificazione dei dati



Registro dei trattamenti (art. 30 GDPR)

- Strumento di censimento dei trattamenti
- Strumento di valutazione e analisi del rischio
- Strumento probatorio avanti l'Autorità

Quando il Registro è obbligatorio?

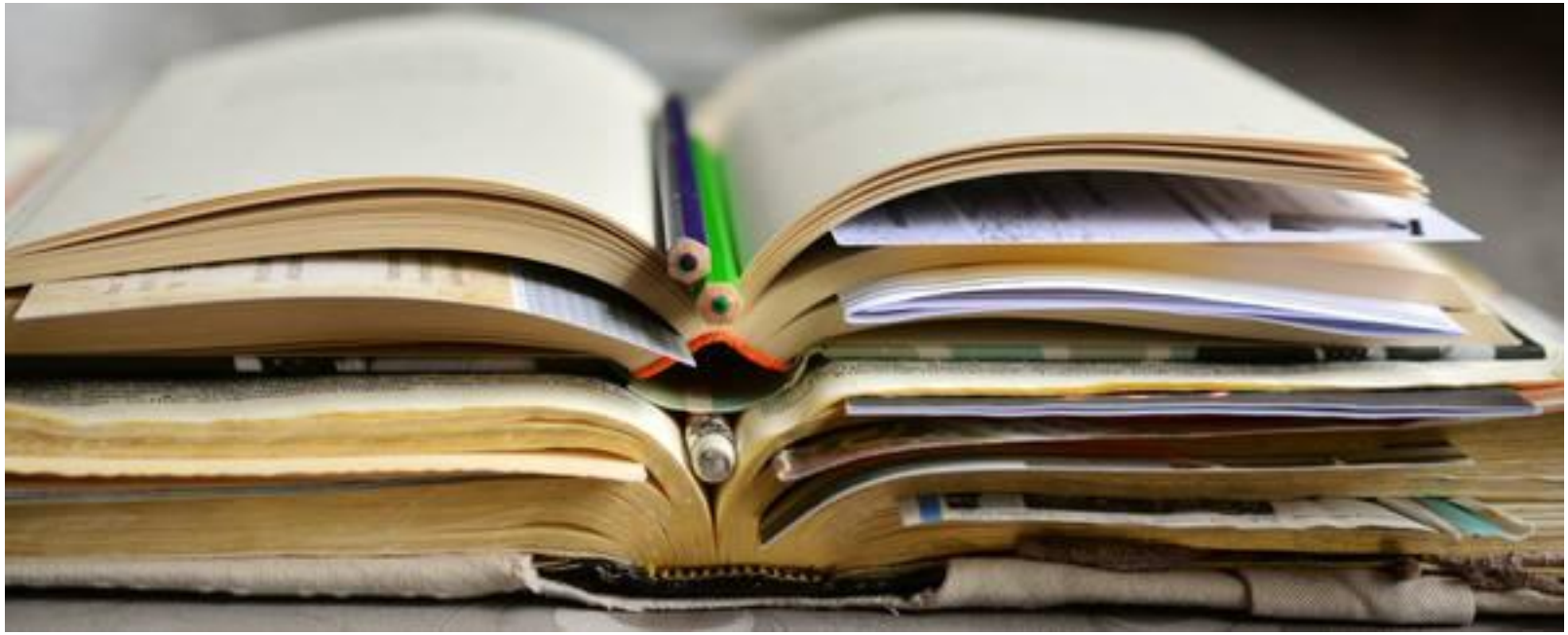
Imprese e organizzazioni **con più di 250** dipendenti

E, IN OGNI CASO, QUALORA IL TRATTAMENTO:

1) presenti un rischio per i diritti e le libertà dell'interessato;
2) non sia occasionale;
3) includa particolari categorie di dati (es. dati i c.d. sensibili) o dati relativi a condanne penali.

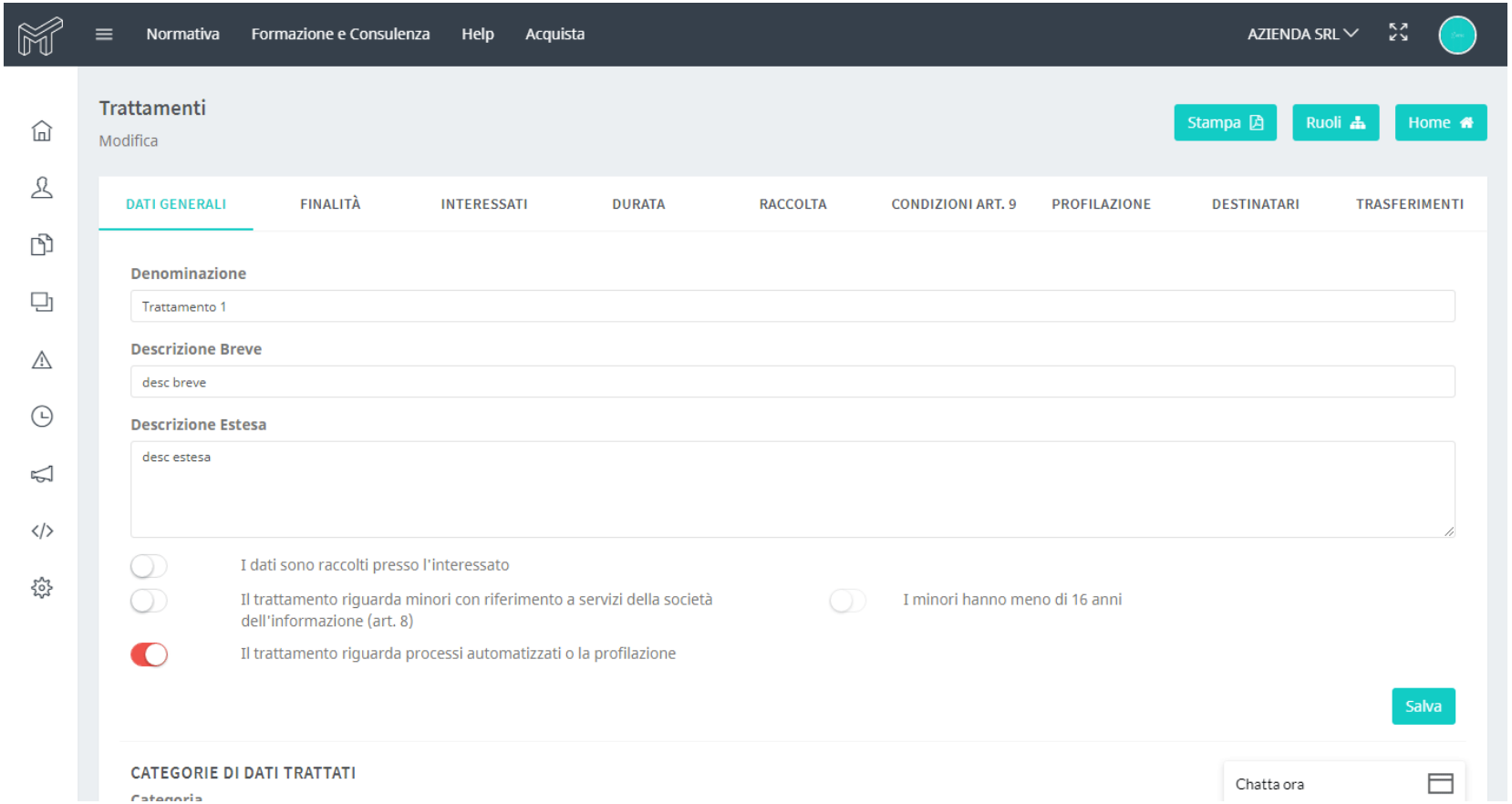
In ogni caso, è sempre consigliabile in quanto assolve al dovere **PROBATORIO** e permette di tenere sempre **MONITORATO** il flusso dei trattamenti

Che caratteristiche deve avere?



Innanzitutto deve essere FACILE DA CONSULTARE

Che forma deve avere?



Adeguato alla realtà aziendale

GDPR - Art.30, comma1, lett.a)		DESCRIZIONE ATTIVITA' DI TRATTAMENTO GDPR - Art.30, comma1, lett.b)	GDPR - Art.30, comma1, lett.c)		GDPR - Art.30, comma1, lett.d)	GDPR - Art.30, comma1, lett.e)	GDPR - Art.30, comma1, lett.f)
AREA	**ATTIVITA' DI TRATTAMENTO**	**FIANLITA'**	**CATEGORIE DI DATI PERSONALI**	**CATEGORIE DI INTERESSATI**	**AMBITO DI COMUNICAZIONE**	**TRASFERIMENTI INTERNAZIONALI**	**TEMPO DI CONSERVAZIONE**
RISORSE UMANE	**Selezione**	Raccolta CV, verifica titolo di studio, verifica certificazioni professionali, verifica esperienze di lavoro pregresse, verifica categorie protette e disabilità, verifica casellario giudiziario (per posizioni apicali)	Anagrafici/codice fiscale, dati idonei a profilare, copie doc.identità, dati di salute. dati giudiziari	Candidati	Nessuno	Nessuno Extra UE calusole adeguatezza	Commisurato finalità (di norma 1 anno)
	Assunzione	Attivazione iter assunzione, gestione contratto, check-list adempimenti normativi-tributari-fiscali-bancari, lul	Anagrafici/codice fiscale, dati idonei a profilare, copie doc.identità, dati di salute, dati giudiziari	Dipendenti, parenti affini o conviventi, minori	Agenzie del lavoro, società recruiting, università, enti competenti, consulenti lavoro	Nessuno Extra UE garanzie contrattuali	Commisurato finalità (2 anni dopo la cessazione del rapporto di lavoro)
	Rilevazione presenze	Gestione accentrata delle timbrature effettuate tramite badge	Anagrafici, dati relativi all'ubicazione	Dipendenti, collaboratori	Consulente lavoro	Nessuno Extra UE norme vincolanti d'impresa	Commisurato finalità (1 anno)
	Integrazione presenze (permessi, infortuni, malattie, maternità, mutue, 104, ecc.)	L'inserimento dei giustificativi rispetto a permessi, ferie, ecc. viene effettuata in forma autonoma dai singoli dipendenti attraverso le aree riservate	Anagrafici, salute, sindacali	Dipendenti, collaboratori	Consulente lavoro, agenzie del lavoro, enti competenti	Nessuno	Commisurato finalità ed obblighi di legge
	Gestione paghe	Cedolini elaborati da studio esterno, archiviati in payroll e scaricati autonomamente dai singoli dipendenti	Anagrafici, economici, salute, appartenenze sindacali, parenti affini e conviventi, minori	Dipendenti, collaboratori	Consulente lavoro, agenzie del lavoro, enti competenti	Nessuno	Commisurato finalità ed obblighi di legge

2° STEP: ANALISI DEI RISCHI ED EVENTUALE VALUTAZIONE DI IMPATTO

I trattamenti di dati personali possono comportare dei **rischi per i diritti e le libertà delle persone fisiche** e cagionare **danni fisici, materiali ed immateriali.**

Quali sono i **rischi** connessi al trattamento **rilevanti ai fini del GDPR**:

1) Discriminazione;
2) Furto o usurpazione d'identità;
3) Perdite finanziarie;
4) Pregiudizio alla reputazione;
5) Perdita del controllo sui propri dati personali;
6) Trattamento di dati sensibili;
7) Trattamenti di dati di soggetti vulnerabili (in particolari minori);
8) Profilazione automatizzata;
9) Etc…

… IN CONCRETO

Vanno analizzate:

- la probabilità che il rischio si verifichi, e
- la gravità delle conseguenze per l'interessato

secondo i seguenti criteri :

- la natura del trattamento (es. automatizzato, manuale, etc.)
- l'ambito di applicazione (es. quali categorie di soggetti trattano i dati, numero di soggetti interessati, etc.)
- Il contesto e le finalità del trattamento

tenendo presente che è richiesta una valutazione oggettiva con cui stabilire se i trattamenti comportano un rischio, **e se tale rischio sia elevato**

Il GDPR fornisce alcuni esempi di trattamenti che possono presentare un **rischio elevato**:

1) **valutazioni sistematiche** e **globali** di aspetti personali basate su un **trattamento automatizzato** compresa la **profilazione**;
2) trattamenti, su **larga scala**, di categorie particolari di dati personali (art. 9 GDPR) o di dati relativi a condanne penali e a reati;
3) **sorveglianza sistematica** su larga scala di una zona accessibile al pubblico.

Le Linee guida del WP29 precisano che non si tratta di un elenco esaustivo.

Se un tipo di trattamento può presentare un rischio elevato

"Valutazione d'impatto" sulla protezione dei dati (DPIA) ex art. 35 GDPR

DI COSA SI TRATTA ?

- ✓ è un **processo** volto a descrivere i trattamenti, valutarne la necessità e proporzionalità in relazione alla finalità del trattamento, aiutare a valutare gli eventuali rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento e determinando le misure previste per affrontarli;

- ✓ deve essere effettuata dal Titolare (con l'aiuto del DPO) prima del trattamento, nel rispetto dei principi di privacy by design e by default;

- ✓ va aggiornato ogni 3 anni.

9 criteri per stabilire se il trattamento può presentare un **rischio elevato** e quindi necessita di eseguire la DPIA, tra questi:

- ✓ Trattamento di dati relativi a **interessati vulnerabili** (es. **minori**, pazienti, dipendenti) ovvero nei casi in cui c'è uno squilibrio nella posizione tra gli interessati e il Titolare, in quanto le persone potrebbero essere **incapaci di opporsi** al trattamento ed esercitare i propri diritti

Le aziende del settore Toys & Kids saranno probabilmente tenute ad effettuare la DPIA se entreranno nel mercato degli Smart Toys o se integreranno dispositivi IoT nei loro prodotti

3° STEP: SCELTA DELLE MISURE PER ATTENUARE I RISCHI

Il Titolare ed il Responsabile del trattamento

devono mettere in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza parametrato al rischio

(non più «*misure minime*» ma «*misure proporzionate al rischio*»)

L'adeguatezza delle misure di sicurezza adottate potrà essere attestata dall'adesione a **codici di condotta** o a **meccanismi di certificazione** (oggi non ancora regolamentati)

Il Regolamento contiene una mera elencazione **aperta** e **non esaustiva** di misure tecniche e organizzative

1) Pseudonimizzazione e cifratura dei dati personali;
2) Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
3) Capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
4) Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure al fine di garantire la sicurezza del trattamento
5) Etc….

La migliore misura di sicurezza rimane sempre il buon senso

Per valutare l’**adeguatezza del livello di sicurezza dei dati** si tiene conto dei rischi presentati dal trattamento che derivano in particolare da:

- Distruzione
- Perdita
- Modifica
- Divulgazione non autorizzata
- Accesso illegale

4° STEP: ATTUAZIONE DI MISURE TECNICHE E ORGANIZZATIVE ADEGUATE

- ✓ Audit interni (almeno ogni 6 mesi)
- ✓ Attività di formazione alle figure apicali e agli incaricati del trattamento
- ✓ Adozione di linee guida e modelli organizzativi interni all'azienda
- ✓ Controllo costante e revisione periodica dei processi (con coinvolgimento diretto delle figure apicali)
- ✓ Codici di condotta e certificazioni (art. 40 e 42 GDPR)

Oggi in Italia non esistono enti in grado di rilasciare certificazioni di trattamenti in conformità al GDPR e non sono ancora stati individuati i criteri per l'approvazione di Codici di condotta

DPO – Data Protection Officer (art. 37 GDPR)

La nomina del DPO avviene su iniziativa del Titolare → Atto di Accountability

Chi è tenuto a nominare un DPO?

- ✓ Autorità pubbliche o ente pubblici;
- ✓ Chi svolge un'attività che richiede il controllo regolare e sistematico degli interessati;
- ✓ Chi tratta su larga scala categorie particolari di dati personali o dati relativi a condanne penali o reati.

! In ogni caso è opportuno valutare l'opportunità di una eventuale **nomina facoltativa** anche laddove non vi sia un obbligo normativo

Compiti del DPO:

- ✓ Raccordo con Autorità Garante e Interessati
- ✓ Parere sulla DPIA
- ✓ Vigilanza e consulenza

Requisiti per la nomina a DPO:

- ✓ Indipendenza;
- ✓ Conoscenze specialistiche sia della normativa che della prassi;
- ✓ Assenza di conflitti di interessi;
- ✓ Nessuna necessarietà di attestati o riconoscimenti formali

- FOCUS SUL SETTORE TOYS & KIDS

Perché i dati dei minori meritano maggior tutela?

Considerando 38 GDPR → I minori meritano specifica protezione dei loro dati in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia, nonché dei loro diritti in relazione alla protezione dei dati. Tale specifica protezione, dovrebbe riguardare in particolare l'utilizzo dei dati dei minori ai fini di **marketing** e **profilazione**

Approccio e metodo

Il Titolare che tratta **dati di minori** dovrebbe:

- ✓ tenere sempre in considerazione il diritto alla protezione dei dati nella fase di sviluppo e progettazione dei propri prodotti/servizi;

- ✓ valutare sempre l'opportunità di eseguire una DPIA (es. se il trattamento comporta l'utilizzo di nuove tecnologie e può rappresentare un rischio elevato per i diritti del minore);

- ✓ Adottare un comportamento volto alla trasparenza e corretta informazione nei confronti dei minori:

  - informarli sempre circa le finalità del trattamento;
  - informarli su come possono esercitare i loro diritti (es. cancellazione);
  - informarli su quali possono essere i rischi che corrono e come prevenirli.

Il consenso come base giuridica per l'utlizzo dei dati dei minori (art. 7 GPRD)

- ✓ Occorre che sia espresso;
- ✓ Deve essere informato (ovvero preceduto dall'informativa);
- ✓ Collegato a determinata o determinate finalità;
- ✓ Se il consenso è prestato all'interno di una dichiarazione scritta che riguarda altre questioni, occorre che il consenso sia distinguibile dalle altre questioni e in forma comprensibile e facilmente accessibile, con un linguaggio chiaro e semplice, altrimenti non è vincolante;
- ✓ Deve essere libero e non condizionato.

Revoca del consenso (art. 7 GDPR)

L'interessato ha il diritto di revocare il proprio consenso

in qualsiasi momento

La revoca **non è retroattiva**, infatti:

"*La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò*".

Quanto alla **forma**:

"*il consenso è revocato con la stessa facilità con cui è accordato*"

Offerta diretta di servizi digitali ai minori

Consenso dei **minori** per i servizi della società dell'informazione (es. gaming on-line, social network, etc.) - ex art. 8 GDPR

Minori > di anni16 → il trattamento dei dati è **lecito**

Minori < di anni16 → Il trattamento dei dati è lecito solo se viene prestato o autorizzato il consenso da parte del **titolare della responsabilità genitoriale**

Gli stati membri possono stabilire per legge un'età inferiore per imporre la necessarietà del consenso purché questa **non sia inferiore ai 13 anni**

Offerta diretta di servizi digitali ai minori #2

La verifica del consenso rilasciato dal minore o la verifica dell'effettiva titolarità della responsabilità genitoriale dovrebbe seguire un approccio proporzionato in base al rischio e in considerazione delle tecnologie disponibili

Rischio basso → potrebbe essere sufficiente una verifica via e-mail

Rischio elevato → Verifiche più approfondite (es. consenso del genitore accompagnato da transazione di pagamento di Euro 0,01 al Titolare del trattamento)

N.B. In ogni caso il Titolare del trattamento non dovrebbe adottare misure di verifica del consenso che prevedano la raccolta eccessiva di ulteriori dati

Offerta diretta di servizi digitali ai minori #3

Alcune questioni aperte

1) Come si deve regolare il trattamento e la raccolta del consenso dei minori in caso di vendita di servizi digitali su mercati UE che hanno adottato una diversa soglia di età in relazione consenso digitale (13-16 anni)?
2) Come bilanciare il principio di minimizzazione dei dati e l'ulteriore richiesta del consenso dell'ex-minore (una volta "scaduto" il consenso del genitore)?
3) 88% dei giocattoli viene comprato da adulti e i relativi siti web sono rivolti ad essi → in tal caso si applicano le regole relative al consenso dei minori per servizi digitali?

Diritti degli interessati nel caso di minori

1) Trasparenza e modalità di trattamento (art. 12 GDPR)

Nel caso di informazioni destinate specificatamente a minori, il Titolare deve adottare una forma **concisa**, **trasparente**, **intelligibile e facilmente accessibile**, con un **linguaggio semplice e chiaro.**

2) Diritto alla cancellazione dei dati ("diritto all'oblio") (art. 17 GDPR)

L'interessato può chiedere la cancellazione dei dati in caso di revoca del consenso al trattamento. Se il consenso è stato rilasciato dal minore (e quindi senza la piena consapevolezza dei rischi) il diritto alla cancellazione **è sempre garantito**, anche se viene esercitato quando il soggetto non è più minore (Considerando 65 GDPR).

Cosa si intede con profilazione?

Definizione ex art. 4 GDPR

"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"

Profilazione basata sul processo decisionale automatizzato (art. 22 GDPR)

L'interessato ha il diritto di **NON** essere sottoposto a una decisione che valuti aspetti personali che lo riguardano, che sia basata **unicamente** su un trattamento **automatizzato** e che produca **effetti giuridici** o incida in modo **significativo** sulla persona (es. rifiuto automatico concessione credito on-line o pratiche di assunzione elettronica senza interventi umani).

Tale trattamento è tuttavia consentito **se previsto dalla Legge, se necessario per la conclusione o esecuzione di un contratto o se è stato rilasciato il consenso**. In ogni caso deve essere previsto il diritto di ottenere l'intervento umano e il diritto di poter esprimere la propria opinione e di contestare la decisione.

TALE MISURA NON DOVREBBE RIGUARDARE UN MINORE (Considerando 71 GDPR)

E’ dunque possibile profilare i minori?

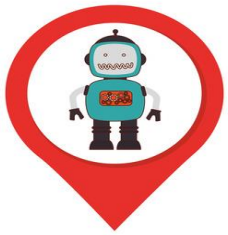
Il **Regolamento** non impone un divieto assoluto alla profilazione dei minori, ma il Titolare deve porre in essere tutte le misure adeguate per la protezione dei loro dati e, dunque:

- ✓ Assicurare il diritto all’intervento umano;
- ✓ Assicurare il diritto di contestare la decisione ed esprimere la propria opinione;
- ✓ Rendere l’accesso a tali diritti “*a misura di bambino*” (di facile utilizzo e comprensibile);
- ✓ Informare l’interessato minore di tale processo decisionale automatizzato.

WP29 ⟶ Sconsiglia di effettuare profilazione su minori per finalità di marketing

Suggerimenti del Garante in tema di Smart-Toys

Gli **smart-toys** sono quei giocattoli capaci di interagire (microfoni, telecamere, sensori) con le persone e con l'ambiente circostante e di connettersi all rete per navigare *on-line* e comunicare con smartphone, tablet, pc o altri smart toys



Gli smart-toys sono quindi in grado di raccogliere, elaborare e comunicare dati e informazioni, con possibili **rischi per la protezione dei dati dei minori**

Suggerimenti del Garante in tema di Smart-Toys

Alcuni consigli per le aziende (e per i consumatori):

1) Prevedere un'informativa completa nella confezione e/o pubblicato sul sito dell'azienda;
2) Prevedere la possibilità di limitare la raccolta e la memorizzazione ai soli dati necessari per il funzionamento del giocattolo
3) Prevedere l'applicazione di adeguate misure di sicurezza per la connessione a Internet degli smart toys da parte dei consumatori (es. password complesse)
4) Prevedere la possibilità di disconessione dalla rete in caso di inutilizzo e di disattivazione dell'account e cancellazione dei dati in caso di vendita, cessione o smaltimento del giocattolo
5) In ogni caso, prevedere la configurazione degli smart-toys per ridurre al minimo la raccolta e il trattamento dei dati (rispetto dei principio di *privacy by default*)

UNO QUATTRO
STUDIO LEGALE

GRAZIE PER L'ATTENZIONE!

AVV. CORRADO BLANDINI
c.blandini@unoquattro.it

AVV. UMBERTO LOCATELLI
u.locatelli@unoquattro.it

Via G. B. Pergolesi 1
20134 Milano (MI)
Tel. 02/2506.1262 – Fax 02/9475.4828
www.unoquattro.it