PROTEZIONE DEI DATI

Quanto di seguito riportato rappresenta solo una precisazione ed un ampliamento di quanto riportato nelle slide.

SLIDE 3
La materia è disciplinata dal Regolamento (UE) 2016/679 entrato in vigore il 25 maggio del 2018 e che ha avuto più di 2 anni di gestazione.
In quanto regolamento , diversamente dalla direttiva, disciplina direttamente tutta la materia e viene recepito così com'è da tutti gli stati membri della C.E.

Precedentemente la materia era disciplinata dal decreto legislativo 196/2003, conosciuto come "codice privacy" e che il legislatore italiano ha scelto di non cancellare (abrogare) totalmente il decreto, ma solo alcune sue parti, tenendo in vita le parti (gli articoli) che trattano la materia in modo simile al regolamento (UE) 2016/679.

Questa scelta è stata dettata da:
1. scelte politiche non meglio specificate
2. motivi tecnici – gli illeciti penali in materia di privacy (ma in generale tutta la materia del diritto penale) sono di competenza dello stato nazionale. Stesso discorso per le materie normate dal diritto fiscale
3. alcune norme nazionali erano molto simili a quelle previste dal regolamento europeo.

Non è stata cancellata la direttiva 2002/58 sul trattamento dati comunicazioni elettroniche, anche se dovrà essere profondamente rivista.

Il 2016/679 si applica solo alle persone fisiche e non anche alle persone giuridiche.
https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali

SLIDE 5
L'art. 4 del regolamento costituisce una sorta di dizionario che definisce il significato dei termini utilizzati dalla norma, al fine di scongiurare ogni sorta di equivoci.

Le definizioni riportate nella slide saranno richieste **a memoria in sede di esame**.

Dato personale: si pone l'accento su "identificata" o "identificabile". Riferita a persona fisica anche chiamata "**interessato**".
E' una definizione molto ampia, è dato personale anche la geolocalizzazione e la password, secondo la definizione.

Trattamento: sono inseriti una serie di esempi con la parola "come" . Sono solo esempi, per cui, se qualcosa non rientra nella seconda parte della definizione (quella delle esemplificazioni), è comunque un trattamento/operazione.

Dati sensibili: all'interno del concetto generale di dato personale viene considerata una "categoria particolare/speciale" dei dati personali.

Dati giudiziari: sono dati solo in ambito di diritto penale. Riguardano i processi in corso, i reati e le misure di sicurezza.

Dati personali è un genus all'interno del quale ci sono i *dati personali identificativi* e gli **ex dati sensibili** e gli **ex dati giudiziari** della direttiva 2002/58.

I dati sensibili ed i dati giudiziari sono un elenco tassativo. L'elenco dei dati sensibili riguarda 3 filoni:

- razza
- pensiero
- dati fisici

https://www.garanteprivacy.it/home/diritti/cosa-intendiamo-per-dati-personali

Informativa all'interessato
SLIDE 9
per esempio l'informativa sulla privacy che firmiamo quando sottoscriviamo un accordo on line.
SLIDE 10
punto a) chi è il soggetto che mi sta chiedendo i dati

Il trattamento dei dati può avvenire anche all'esterno della Comunità Europea. Per esempio negli Stati Uniti, dove i dati di privacy non sono molto tutelati, esiste un ente che elenca le società che garantiscono una situazione di tutela dei dati personali.

l trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
=> Articolo: 13, 21
=> Motivo: 113, 47, 48

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Trattamento lecito
SLIDE 19
Art .6 – adempiere obbligo legale: per es. raccolta di dati personali (codice fiscale) per emetter la fattura; ancora la raccolta di dati personali in ambito medico, softspam (invio di comunicazioni promozionali mediante e-mail o posta tradizionale a clienti per pubblicizzare prodotti e/o servizi analoghi a quelli già in precedenza acquistati dal destinatario) rientra nel caso di legittimo interesse del titolare nel promuovere la propria merce presso già clienti.

Consenso
SLIDE 21.
Atto positivo inequivocabile –

- significa che deve esserci un comportamento attivo, non è permessa la preselezione delle caselle di accettazione

SLIDE 22
Punto 1 …….*"in grado di dimostrare"*…….= meglio in forma scritta.

Principio innovativo/inyterpretativo
SLIDE 24 – Art. 24.

Viene introdotto il concetto di **ACCOUNTABILITY** – termine inglese che fa emergere una particolare metodologia interpretativa anglosassone del diritto.

Invece di fornire un elenco di cose da fare o da non fare la norma attribuisce al titolare del trattamento dei dati la **RESPONSABILITA**' di applicare (e quindi di provare di aver applicato) misure tecnico/organizzative adeguate per la raccolta, il trattamento, la conservazione dei dati.

E' un termine difficile da definire sinteticamente poiché è un insieme di caratteristiche

compliance – conformità normativa.

SLIDE 28
Titolare è colui che decide su metodi e finalità della raccolta e conservazione dei dati personali.
Deve dimostrare che le misure tecniche/organizzative sono adeguate.
Passaggio chiave è di essere in grado di aver adottato misure "ADEGUATE" , quindi non più minuziosamente elencate e descritte dal legislatore.
Queste regole iperprecise erano richieste nel vecchio regime, a tutti intitolari, indipendentemente dalle loro dimensioni(GOOGLE o il piccolo imprenditore erano equiparati).
Vecchie norme fornivano i singoli fatti
Nuove norme danno indirizzi generali entro cui stare e le misure da adottare non sono universali , ma devono essere commisurate alle singole situazioni: una cosa è google che raccoglie, tratta e conserva immensa mole di dati, un'altra è la piccola azienda che raccoglie tratta e conserva i datio personali dei sui 2 dipendenti.

L'organo ispettivo deputato al controllo delle norme sul trattamento dei dati personali è la Guardia di Finanza.

Soggetti che effettuano il trattamento dei dati
SLIDE 31
Titolare del trattamento
Contitolari del trattamento art. 29 del regolamento europeo – parola chiave "congiuntamente" - "accordo di contitolarità"che determina la suddivisione dei compiti per esempio tra raccolta e conservazione dei dati.
Responsabile del trattamento – magari titolare di un contratto di consulenza di un professionista informatico non "dipendente" - per definire il contratto in questo caso è necessaria la forma scritta (ad substantiam).Incaricato – nella nuova normativa la parola incaricato non c'è più, ma l'articolo recita…….e dà una versione più generica della figura tipica del lavoratore dipendente.
Il datore di lavoro deve istruire il proprio dipendente.
Responsabile per la protezione dei dati – obbligatorio in 3 casi – è una figura autonoma e collaborativa, non solo inquisitoria. E' figura di vigilanza interna o esterna alla struttura, è l'incaricato per i rapporti con l'autorità giudiziaria ma non è suo sostituto.
Il DPO è un **consulente esperto** che va ad affiancare il titolare nella gestione delle problematiche del trattamento dei dati personali, in tal modo garantendo che un soggetto qualificato si occupi della materia, aggiornandosi sui rischi e le misure di sicurezza, in considerazione della crescente importanza e complessità del settore
La designazione del DPO riflette il nuovo approccio del regolamento europeo (art. 39), maggiormente responsabilizzante, essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare e del responsabile. **Il ruolo del DPO è di tutelare i dati personali, non gli interessi del titolare del trattamento.** E ciò appare ovvio soprattutto nell'ambito degli enti pubblici e delle aziende che effettuano un monitoraggio su larga scala degli individui. Il DPO deve, infatti, possedere un'adeguata conoscenza delle normative e delle prassi di gestione dei dati personali, e **deve adempiere alle proprie**

funzioni in piena autonomia ed indipendenza, e in assenza di conflitti di interesse. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici aziendali, quindi in grado di influenzare le scelte adottate in materia di trattamento dei dati. Se l'attività principale consiste nel trattamento su larga scala di dati sensibili, relativi alla salute, alla vita sessuale, genetici, giudiziari e biometrici. Il monitoraggio del comportamento delle persone interessate comprende tutte le forme di monitoraggio e profilazione su Internet, anche ai fini della pubblicità comportamentale.

Ad esempio, una palestra o una catena di palestre, trattando dati relativi alla salute potrebbe avere la necessità di nominare un DPO.

Come si può notare, è raro che una azienda di piccole o medie dimensioni abbia l'obbligo di nominare un DPO, ma è anche vero che oggi esistono aziende di piccole dimensioni che comunque trattano grandissime quantità di dati, grazie a strumenti informatici. Gli esempi possono essere parecchi, come un call center, oppure un centro commerciale che ha un impianto di videosorveglianza e che rientra nell'ipotesi di cui al numero 2.

Le autorità di controllo raccomandano ai titolari e responsabili di effettuare una valutazione in merito all'obbligo o meno di nominare il DPO, documentando tale valutazione compiuta (ad esempio all'interno del registro dei trattamenti). funzioni in piena autonomia ed indipendenza, e in assenza di conflitti di interesse. In tal senso non può ricoprire tale incarico un soggetto che si trova ai vertici aziendali, quindi in grado di influenzare le scelte adottate in materia di trattamento dei dati.

Proprio per garantire l'autonomia del DPO, l'articolo 38 del GDPR stabilisce che il titolare del trattamento e il responsabile del trattamento si assicurano che il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Inoltre, il DPO non può essere rimosso o penalizzato dal titolare o dal responsabile del trattamento per l'adempimento dei propri compiti. In tal senso appare difficile ritenere che tale autonomia sia giustificabile nell'ambito di un rapporto di lavoro dipendente, per cui sarebbe preferibile che il DPO sia un soggetto esterno. Ovviamente, titolare e responsabile devono mettere a disposizione del DPO le risorse umane e finanziarie per poter svolgere il suo compito.
Il ruolo di DPO può essere affidato ad uno dei dipendenti dell'azienda ma può anche essere esternalizzato a un fornitore di servizi (libero professionista o azienda) tramite apposito contratto, nel qual caso dovrà essere nominato anche responsabile del trattamento. È difficilmente immaginabile, infatti, che possa svolgere le sue funzioni senza avere accesso ai dati personali. Può essere una persona fisica o un’organizzazione, e può essere nominato per un gruppo di imprese al fine di ridurre i costi.
Tale designazione è obbligatoria solo in tre casi.

1) Per le amministrazioni e gli enti pubblici (eccetto le autorità giudiziarie nell'esercizio delle loro funzioni). Nel regolamento europeo non vi è una definizione di "autorità pubblica", per cui occorrerà interpretare l'indicazione in base al diritto nazionale.

Se l'**attività principale** svolta dal titolare o dal responsabile del trattamento consiste nel trattamento di dati che per la loro natura, oggetto o finalità, richiedono il **controllo regolare e sistematico degli interessati** su larga scala.

Con riferimento all'**attività principale**, il Gruppo di lavoro articolo 29 precisa che occorre tenere presente il legame del "core business" con l'attività di trattamento dati. Anche se l'attività principale di un **ospedale** non è il trattamento dei dati ma la salute dei pazienti, essendo le due attività strettamente collegate, il trattamento dei dati rientrerà nell'alveo delle attività principali, per cui un ospedale dovrà nominare un DPO. Stesso discorso si può fare per una **società di vigilanza**, dove l'attività di sorveglianza è indissolubilmente legata all'attività di trattamento dei dati personali relativi, e quindi per un'assicurazione, una banca od un call center. Di contro, anche se nella pratica tutte le imprese trattano dati (es. i pagamenti dei dipendenti), non rientrano nell'obbligo di nomina del DPO se il trattamento dei dati è solo di supporto al "core business".

La nozione di **monitoraggio regolare e sistematico** include non solo tutti i vari strumenti di tracciatura elettronica e profilazione online, ma anche qualsiasi forma di tracciatura in un ambiente offline. Per il WP29, un **monitoraggio è regolare** se avviene di continuo o in un arco temporale ben definito, se ripetuto ad intervalli constanti. Il **monitoraggio è sistematico** se si verifica in base ad uno schema o quando è organizzato, metodico, prestabilito, o se rientra in un piano generale od una strategia (es. servizi di telecomunicazione, marketing, geolocalizzazione, fidelizzazione, monitoraggio di dati sulla salute e forma fisica attraverso dispositivi indossabili, reindirizzamento di email).

Per stabilire se un **trattamento è su larga scala** il WP29 suggerisce di tenere in considerazione alcuni elementi:
- il numero degli interessati coinvolti (in termini assoluti o in percentuale rispetto alla popolazione di riferimento);
- la quantità dei dati trattati;
- le diverse tipologie di dati trattati;
- la durata del trattamento;
- la portata geografica del trattamento.

In tal senso sono trattamenti su larga scala quello dei dati di viaggio dei soggetti che usano un sistema di trasporto pubblico (es. il monitoraggio tramite carte di viaggio), il trattamento dei dati dei pazienti da parte di un ospedale, il

trattamento di dati di geolocalizzazione della clientela per fini statistici, il trattamento dei dati dei clienti di una banca o un'assicurazione, il trattamenti dei dati personali per la pubblicità comportamentale (tramite cookie di profilazione), il trattamento di dati dei fornitori di servizi telefonici o internet, i trattamenti operati tramite fidelity card (a meno che non si tratti di un piccolo negozio). Non sono trattamenti su larga scala quelli del singolo medico o del singolo avvocato.
3)Se **l'attività principale consiste nel trattamento su larga scala** di dati sensibili, relativi alla salute, alla vita sessuale, genetici, giudiziari e biometrici. Il monitoraggio del comportamento delle persone interessate comprende tutte le forme di monitoraggio e profilazione su Internet, anche ai fini della pubblicità comportamentale.
Ad esempio, una palestra o una catena di palestre, trattando dati relativi alla salute potrebbe avere la necessità di nominare un DPO.

Come si può notare, è raro che una azienda di piccole o medie dimensioni abbia l'obbligo di nominare un DPO, ma è anche vero che oggi esistono aziende di piccole dimensioni che comunque trattano grandissime quantità di dati, grazie a strumenti informatici. Gli esempi possono essere parecchi, come un call center, oppure un centro commerciale che ha un impianto di videosorveglianza e che rientra nell'ipotesi di cui al numero 2.
Le autorità di controllo raccomandano ai titolari e responsabili di effettuare una **valutazione in merito all'obbligo o meno di nominare il DPO**, documentando tale valutazione compiuta (ad esempio all'interno del registro dei trattamenti).

Registro delle attività di trattamento.
E’ un riassunto schematico del trattamento effettuato del dato.
Tale registro è centrale e l’obbligo ricade sul titolare del trattamento e sul responsabile del trattamento. Se le 2 figure sono ricoperte da un unica persona devono comunque essere tenuti entrambi i registri.
Al di là della numerosità di 250 dipendenti le caratteristich precisate nel prosieguo del del punto 5 fanno sì che anche aziende minori siano tenute a tale obbligo.
Si tenga per esempio presente che anche una piccola azienda con pochi dipendenti chiede per la loro assunzione l’estratto del casellario giudiziario dei dati del dipendente.
Il registro deve riportare le categorie di dati trattati (personali, sensibili, giudiziari), (f) la durata della conservazione dei dati, (g) le metodologie adottate per la salvaguardia dei dati personali.
I registri devono essere tenuti sempre in forma scritta o anche elettronica con firma digitale.