ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

Conseguenze e problematiche:
sanzioni, data breach, trattamento di dati nella fase di assunzione e nel rapporto di lavoro

Protezione dei dati personali in pratica

Cesare De Santis/Paola Borghi

Roma 29/04/2022

Agenda

- Presentazione relatore
- Protezione dei dati personali in pratica
- Bibliografia & sitografia
- Q&A

Agenda

- **Presentazione relatore**
- Protezione dei dati personali in pratica
- Bibliografia & sitografia
- Q&A

Presentazione relatore (1/2)

Cesare De Santis

Ho lavorato a lungo per Enti della P.A. (Difesa/Aeronautica) ed aziende private (banca e alcune società di consulenza di emanazione bancaria) prima di intraprendere, nel 2008, un autonomo percorso professionale.

Attualmente sono amministratore unico di PRIMAe srl a socio unico, che opera principalmente sui temi della conformità normativa e della protezione dei dati personali. Tra i clienti di PRIMAe srl si annoverano associazioni bancarie, banche, finanziarie, rappresentanze italiane di compagnie di assicurazione europee, altre società di consulenza. Assicuriamo il servizio DPO ad alcune banche.

Titoli/certificazioni/attestati

Laureato in Scienze statistiche ed attuariali, abilitato alla professione di attuario, CISM, iscritto nel registro dei consulenti privacy di KHC (http://www.khc.it/)

Presentazione relatore (2/2)

Paola Borghi

Sono componente della Commissione di certificazione dell'Università Roma Tre; svolgo attività di consulenza prevalentemente in tema di tutela dei dati personali.
Ricopro il ruolo di Data Protection Officer (DPO) di alcune aziende bancarie e assicurative, nonché della Commissione di certificazione dei rapporti di lavoro dell'Università Roma Tre.
Docente dal 2016, nel Master Universitario "Responsabile della protezione dei dati personali: Data Protection Officer e privacy expert", presso l'Università Roma Tre.
Ho altresì partecipato, come docente, al Progetto formativo Smedata, dedicato a PMI e professioni legali, progetto internazionale curato dal Garante per la protezione dei dati personali finalizzato a garantire l'effettiva applicazione del Regolamento Generale sulla Protezione dei Dati Personali, cofinanziato dalla Commissione Europea nell'ambito del Programma dell'Unione Europea "Rights, Equality and Citizenship".

Agenda

- Presentazione relatore
- Protezione dati personali in pratica
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- **Protezione dati personali in pratica: sanzioni & data breach**
- Q&A
- Bibliografia & sitografia

Sanzioni nel GDPR: amministrative pecuniarie

- La infrazione alle seguenti prescrizioni è soggetta a sanzioni amministrative pecuniarie fino a **10.000.000 € o , per le imprese, al 2% del fatturato mondiale** totale annuo dell'esercizio precedente se più alto:
  - ✓ Obblighi del Titolare/Responsabile conformi agli art. 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42, 43
  - ✓ Obblighi dell'organismo di certificazione conformi agli art. 42 e 43
  - ✓ Obblighi dell'organismo di controllo conformi all'art. 41 c.4
- La infrazione alle seguenti prescrizioni è soggetta a sanzioni amministrative pecuniarie fino a **20.000.000 € o , per le imprese, al 4% del fatturato mondiale** totale annuo dell'esercizio precedente se più alto:
  - I principi base per il trattamento, includendo le condizioni per il consenso conformi agli art. 5, 6, 7, e 9
  - I diritti dei soggetti interessati conformi agli art. da 12 a 22
  - Il trasferimento di dati personali a un destinatario in un Paese terzo o organizzazione internazionale conformi agli art. da 44 a 49
  - Ogni obbligo di conformità alle leggi dello Stato membro adottate a norma del capo IX
  - Non conformità a un ordine o una limitazione temporanea/definitiva sul trattamento o la sospensione di flussi di dati dall'Autorità di controllo conformi agli art 58 c.2 o negato accesso in violazione art 58 c.1
- **Non conformità a un ordine dell'Autorità di controllo** come prescritto all'art. 58 c.2 è soggetto a sanzioni amministrative pecuniarie fino a 20.000.000 € o , per le imprese, al 4% del fatturato mondiale totale annuo dell'esercizio precedente se superiore

Sanzioni nel GDPR: condizioni per imposizione

- Ogni Autorità di controllo garantisce che la imposizione di sanzioni amministrative pecuniarie siano, in ogni singolo caso, **effettive, proporzionate e dissuasive**
- Circostanze che contribuiscono a determinare sanzione pecuniaria:
  - **a) natura, gravità e durata** della violazione considerata natura, oggetto e finalità del trattamento così come numero di soggetti interessati lesi e livello di danno subito
  - **b) carattere colposo/doloso** della violazione
  - c) misure prese da Titolare/Responsabile **per attenuare danno** subito da interessati
  - **d) grado responsabilità** di Titolare/Responsabile considerate le misure tecniche/organizzative messe in atto (artt. 25 e 32)
  - e) eventuali **precedenti violazioni** pertinenti commesse da Titolare/Responsabile
  - f) il **grado di cooperazione** con l'Autorità di controllo, al fine di porre rimedio alla violazione e attenuare possibili effetti negativi
  - g) le **categorie** specifiche di **dati personali** interessati dalla violazione
  - h) la maniera in cui l'Autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il Titolare/Responsabile **ha notificato la violazione**
  - i) qualora siano stati disposti **provvedimenti** (art. 58 c.2) nei confronti Titolare/Responsabile relativamente allo **stesso oggetto** e il rispetto di essi
  - j) adesione a **codici di condotta o meccanismi di certificazione** approvati
  - k) eventuali altri **fattori aggravanti/attenuanti** applicabili
- Se Titolare/Responsabile con dolo o colpa viola per stesse operazioni di trattamento diverse norme del Regolamento **la somma delle sanzioni non può superare l'ammontare della violazione più grave**

Sanzione 1: inadeguatezza del DPO

- **Autorità di controllo** → CNPD (Lussemburgo)
- **Contesto** → audit tematico effettuato in diversi Enti/aziende sul ruolo del DPO
- **Importo sanzione** → 18.000 €
- **Anno** → 2021
- **Contenuti:**

  L'audit si è svolto sui seguenti aspetti:

  ✓ qualità professionali ed esperienza sul campo del DPO

  primo DPO legale ma non conoscitore settore, secondo DPO conoscitore settore, no legale ma supportato da studio legale esterno

  ✓ obbligo di pubblicare i recapiti del DPO

  difficile reperimento su sito (no sezione privacy) informativa privacy in una sola lingua (inglese)

  ✓ il DPO come parte attiva dell'organizzazione

  DPO reattivo (su richiesta) ma non proattivo, coinvolgimento DPO da disciplinare in procedura

  ✓ obbligo di fornire risorse sufficienti al DPO

  elementi da considerare: tempo dedicato al ruolo, accesso alle informazioni delle singole U.O. aziendali

  ✓ il conflitto di interessi

  non pianificata l'analisi dei conflitti di interesse tra due funzioni svolte dalla stessa persona all'interno dello stesso ente

  ✓ il ruolo di controllo del DPO

  non formalizzate procedure di controllo sul tema della protezione dei dati (piano dei controlli del DPO).

- **Tendenze emerse:** Il DPO deve avere almeno tre anni di esperienza

Sanzione 2: conflitto di interesse del DPO

- **Autorità di controllo** → APD (Belgio)
- **Contesto** → intervento Autorità a seguito data breach aziendale
- **Importo sanzione** → 50.000 €
- **Anno** → 2020
- **Contenuti:**

  Nell'ambito di una verifica originata da un *data breach* occorso nell'azienda l'Autorità ha rilevato un conflitto di interesse nella figura del DPO designato che ricopriva anche il ruolo di direttore dei dipartimenti *compliance, risk management e internal audit .*

  In particolare sono state sollevate de questioni:

  a) *la possibilità per il DPO di effettuare audit interni, quale direttore del relativo dipartimento, che possano sfociare nel licenziamento di dipendenti nel caso di performance negativa ciò potrebbe incrinare la fiducia che i dipendenti dell'azienda devono poter riporre nella figura del DPO;*

  b) *l'esistenza di eventuali poteri decisionali in capo al DPO in relazione alle finalità e modalità del trattamento, derivanti dai suoi altri incarichi*

  Si evince quindi che il DPO non deve godere di poteri decisionali rispetto alle scelte che lazienda compie in termini di trattamento dei dati personali (ad esempio quali dati trattare, per quali fini utilizzarli ecc.). Questa circostanza avvicinerebbe la posizione del DPO a quello che è il ruolo proprio del titolare del trattamento e ne comprometterebbe l'indipendenza.

- **Tendenze emerse:** Il DPO non deve avere poteri decisionali rispetto al trattamento dei dati personali.

Sanzione 3: mancata cancellazione massiva dei dati

- **Autorità di controllo** → CNIL (Francia)
- **Contesto** → intervento di controllo dell'Autorità
- **Importo sanzione** → 1.750.000 €
- **Anno** → 2020
- **Contenuti:**

  Nell'ambito di un controllo sul rispetto del GDPR e delle legge francese in materia di protezione dei dati personali, CNIL ha sanzionato una compagnia di assicurazioni anche per non aver rispettato i tempi di conservazione di dati personali dichiarati nelle informative e nel Registro dei trattamenti per le categorie di soggetti clienti potenziali (2 mila soggetti per i quali era stato indicato un tempo di conservazione di 3 anni) e clienti (2 milioni per i quali erano da rispettare le prescrizioni di legge, quali quelle previste nel Codice delle assicurazioni e nel Codice del commercio francesi) il cui contratto era cessato e per i quali erano presenti anche dati sensibili.

- **Tendenze emerse:** Rigorosa osservanza dei tempi di conservazione dichiarati nelle informative privacy e nel registro dei trattamenti

Sanzione 4: marketing illecito sui social network

- **Autorità di controllo** → Garante per la protezione dei dati personali (Italia)
- **Contesto** → controllo su reclamo
- **Importo sanzione** → 5.000 € + ammonimento
- **Anno** → 2021
- **Contenuti:**

Sulla base di un reclamo ricevuto il Garante privacy ha sanzionato una piccola società immobiliare, un cui collaboratore aveva inviato ad un contatto del social network professionale Linkedin (che aveva, a seguito di esso, rivolto reclamo al Garante) un messaggio promozionale finalizzato a proporre servizi immobiliari in riferimento ad uno specifico immobile di proprietà della reclamante.

Di seguito le motivazioni(il grassetto è nostro):

" … Linkedin, in particolare, è una piattaforma che ha come finalità quella di mettere in contatto individui che condividono gli stessi interessi professionali per favorire lo scambio di conoscenze o le opportunità lavorative. ***Non è invece previsto che gli utenti di Linkedin possano utilizzare la piattaforma per inviare messaggi ad altri utenti con lo scopo di vendere prodotti o servizi*** *anche se in ciò consiste, evidentemente, la propria attività lavorativa. In tale contesto, non ha alcuna rilevanza il fatto che il profilo di un utente sia aperto o meno alla ricezione di contatti da parte di altri utenti del network perché ciò che conta è la finalità - in questo caso promozionale - per cui il messaggio è inviato, finalità che è in contrasto con quella, prospettata nelle condizioni contrattuali di adesione al social network, che l'interessato può attendersi …"*

" … Nel caso di specie, dunque, il collaboratore della Società ***ha utilizzato il registro immobiliare e il social network – istituiti per finalità determinate - per proporre un servizio di vendita, finalità diversa e incompatibile con quelle originarie*** *e pertanto non rientrante fra le legittime aspettative dell'interessata …"*

La ***reticenza*** *della società rispetto alle richieste del Garante ha costituito una aggravante che è stata specificatamente sanzionata (mentre l'invio illecito – caso isolato, unico messaggio, piccola dimensione societaria – aveva dato luogo solo ad un ammonimento).*

- **Tendenze emerse:** Ribadita la necessità del rispetto del principio di finalità

Sanzione 5: smarrimento documento

- **Autorità di controllo** → Office of the Commissioner for Personal Data Protection (Cipro)
- **Contesto** → controllo su reclamo
- **Importo sanzione** → 15.000 €
- **Anno** → 2021
- **Contenuti:**
- *L'Autorità per la protezione dei dati personali cipriota ha sanzionato la Bank of Cyprus con 15.000 euro per non aver ottemperato alla richiesta di polizza di un cliente (art. 15 GDPR) non avendo ritrovato il documento. In particolare, l'Autorità ha sottolineato che la banca non ha rispettato gli obblighi previsti dal GDPR perché la perdita della polizza assicurativa del denunciante lo ha privato del diritto di accesso al contratto assicurativo, rendendolo incapace di verificare la correttezza e la validità dei suoi dati e di verificare la liceità del trattamento. Inoltre, l'Autorità ha osservato che la sanzione pecuniaria era dovuta alla mancata comunicazione della violazione dei dati in relazione alla perdita del contratto entro 72 ore (data breach) dal momento in cui la violazione era stata portata a sua conoscenza. Infine, l'Autorità ha dichiarato che Eurolife Ltd, anch'essa presa di mira dal denunciante, che ha agito in qualità di autonomo titolare del trattamento dei dati, non ha trattato illegalmente i dati personali del denunciante.*

- **Tendenze emerse:** Necessità di attenta conservazione della documentazione contrattuale, il cui smarrimento implica *data breach*

Data breach: definizione e linee guida

- «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* (Art. 4 c. 12 e Considerando 85 GDPR).
- Nel GDPR è disciplinata da:
  - Art. 33 *«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 …omissis …»*
  - Art.34 *«**Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, **il titolare del trattamento comunica la violazione all'interessato** senza ingiustificato ritardo … omissis …»*
- La notifica di una violazione di dati personali deve essere inviata (in via preliminare e/o definitiva) al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità
- Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha messo disposizione un apposito strumento di autovalutazione (*self assessment*) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza

Data breach: invio erroneo da parte outsourcer ad altra banca

- Tipo azienda → *Banca*
- Tipologia dati coinvolti → *Dati identificativi e bancari (che non consentono però conoscenza dello stato finanziario dei soggetti interessati)*
- Tipologia interessati coinvolti → *Clienti (persone fisiche)*
- Numerosità interessati → *99 (in 107 record)*
- Modalità di rilevazione evento → *Ticket inviato ad outsourcer da parte di altra banca ricevente il file inviato per errore*
- Descrizione evento → *Per un errore della procedura informatica l'outsourcer, responsabile del trattamento, ha inviato un file di clienti destinato alla banca titolare del trattamento ad un'altra banca*
- Notificazione Garante → *No (vedi anche caso n. 9 «Accidental transmission of data to a trusted third party" della linea guida EDPB)*
- Comunicazione interessati → *No (vedi anche caso n. 9 «Accidental transmission of data to a trusted third party" della linea guida EDPB)*
- Inserimento in Registro violazioni → *Sì*
- Denuncia ad Autorità Giudiziaria → *No*
- Misure di rimedio → *Richiesta di cancellazione del file alla banca ricevente, che ha prodotto altresì dichiarazione di non utilizzo e cancellazione del file*
- Misure di mitigazione effetti → *Correzione da parte outsourcer dell'anomalia al software utilizzato che ha causato l'invio errato*

Data breach: smarrimento documenti cartacei

- Tipo azienda → *Banca*
- Tipologia dati coinvolti → *Dati identificativi (anche copia documenti di identità) e bancari (IBAN), fatture spese mediche, firme autografe su documenti cartacei*
- Tipologia interessati coinvolti → *Una categoria di soggetti interni*
- Numerosità interessati → *<10*
- Modalità di rilevazione evento → *Comunicazione incaricato del trattamento*
- Descrizione evento → *Addetto all'Ufficio del personale dimenticava su un mezzo pubblico cartella contenente copie cartacee di documentazione destinata a rimborsi assicurativi*
- Notificazione Garante → *Si*
- Comunicazione interessati → *Si*
- Inserimento in Registro violazioni → *Sì*
- Denuncia Autorità Giudiziaria → *Sì*
- Misure di rimedio → *Modifica procedura organizzativa*
- Misure di mitigazione effetti → *Lettera banca ai soggetti interessati che offriva chiusura/riapertura gratuita dei rapporti in essere e assicurava rifusione perdite finanziarie attribuibili al data breach*

Data breach: smarrimento telefono cellulare

- Tipo azienda → *Banca*
- Tipologia dati coinvolti → Numeri di telefono, email, messaggi
- Tipologia interessati coinvolti → *Soggetti memorizzati in rubrica, mittenti/destinatari email*
- Numerosità interessati → *<200*
- Modalità di rilevazione evento → *Comunicazione assegnatario dispositivo*
- Descrizione evento → *Telefono cellulare con accesso alla posta elettronica aziendale assegnato a figura apicale azienda veniva smarrito*
- Notificazione Garante → *No (vedi caso 10 «Stolen material storing encrypted personal data» in linea guida EDB)*
- Comunicazione interessati → *No (vedi caso 10 «Stolen material storing encrypted personal data» in linea guida EDB)*
- Inserimento in Registro violazioni → *Sì*
- Denuncia Autorità Giudiziaria → *Sì*
- Misure di rimedio → *PIN SIM e password accesso al dispositivo, crittografia dispositivo, cancellazione da remoto memoria dispositivo*
- Misure di mitigazione effetti → *Procedura organizzativa per adottare cautele nell'uso dei dispositivi aziendali*

Data brach: attacco hacker a server di posta elettronica

- Tipo azienda → *Azienda industriale*
- Tipologia dati coinvolti → *indirizzi email aziendali e dati contenuti in esse*
- Tipologia interessati coinvolti → *dipendenti/collaboratori*, *mittenti/destinatari email*
- Numerosità interessati → *<4.000 (dipendenti/collaboratori)*
- Modalità di rilevazione evento → *Vulnerability assessment effettuato da terza parte*
- Descrizione evento → *Sfruttando vulnerabilità (tecnica shell remota) causata da mancato aggiornamento prodotto antimalware da parte società di manutenzione ignoto attaccante si procurava accesso a server di posta elettronica in via di dismissione senza evidenza di esfiltrazione di dati*
- Notificazione Garante → *Si (richieste ulteriori informazioni da Autorità)*
- Comunicazione interessati → *Effettuata in seguito*
- Inserimento in Registro violazioni → *Sì*
- Denuncia Autorità Giudiziaria → *Effettuata in seguito*
- Misure di rimedio → *Aggiornamento prodotto antimalware, modifica password utenze di posta elettronica,*
- Misure di mitigazione effetti → *Modifica procedura organizzativa verso società di manutenzione e promozione azione risarcitoria verso di essa*

Data breach: attacco *social engineering* a dipendente agenzia banca

- Tipo azienda → *Banca*
- Tipologia dati coinvolti → *Dati identificativi e bancari*
- Tipologia interessati coinvolti → *Clienti (persone fisiche)*
- Numerosità interessati → *2 (clienti banca) + 5 (soggetti esterni alla banca)*
- Modalità di rilevazione evento → *Comunicazione del dipendente*
- Descrizione evento → *Un soggetto esterno alla banca contattava telefonicamente un dipendente di una filiale, presso la quale c'era stato qualche giorno prima un intervento di manutenzione, e qualificandosi come appartenente al reparto di manutenzione della banca otteneva dal dipendente la digitazione del codice di accesso per una piattaforma di assistenza on line ottenendo, in questo modo, l'accesso ed il controllo del PC dal quale disponeva dei bonifici prima che la sua attività venisse bloccata dai tecnici IT della banca avvertiti dal dipendente stesso, resosi conto in ritardo del grave errore commesso.*
- Notificazione Garante → *Sì*
- Comunicazione interessati → *Sì*
- Inserimento in Registro violazioni → *Sì*
- Denuncia ad Autorità Giudiziaria → *Sì*
- Misure di rimedio → *Blocco dell'utenza compromessa, non autorizzazione/richiamo dei bonifici predisposti fraudolentemente, disattivazione della piattaforma di assistenza online utilizzata nell'attacco, cambio di tutte le password dei dipendenti dell'agenzia*
- Misure di mitigazione effetti → *In aggiunta alle iniziative (corso di formazione on line sulla sicurezza e specifici alert su possibili minacce inviati dalla Funzione IT alla rete di agenzie) già intraprese prima del data breach, iniziativa di sensibilizzazione in presenza fisica da parte Funzione Audit presso il personale, offerta chiusura/riapertura gratuita dei conti ai soggetti interessati coinvolti*

Agenda

- Presentazione relatore
- Protezione dei dati personali in pratica
- Q&A
- Bibliografia & sitografia

Agenda

- Presentazione relatore
- **Protezione dati personali in pratica: trattamento dati nel rapporto di lavoro**
- Q&A
- Bibliografia & sitografia

Regolamento (GDPR)

CAPO IX

Disposizioni relative a specifiche situazioni del trattamento

ART. 88

Trattamento dei dati nell'ambito dei rapporti di lavoro

Trattamento dati personali nel rapporto di lavoro

Regolamento

ART. 88

1. *Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro per finalità di*
   - *assunzione*
   - *esecuzione contratto*
   - *gestione, pianificazione e organizzazione*
   - *parità e diversità*
   - *salute e sicurezza*
   - *protezione della proprietà*
   - *cessazione del rapporto*

2. *Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda:*
   - *trasparenza del trattamento*
   - *trasferimento dei dati personali infragruppo*
   - *sistemi di monitoraggio sul posto di lavoro*

La normativa nazionale

D.lgs. n. 196 del 2003 (nuovo testo)

Titolo VIII Trattamenti nell'ambito del rapporto di lavoro

Art. 111 - Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro

Art. 111 bis - Informazioni in caso di ricezione dei curricula

Art. 113 Raccolta di dati e pertinenza

Art. 114 (Garanzie in materia di controllo a distanza)

Art. 115 (Telelavoro, lavoro agile e lavoro domestico)

Privacy e gestione risorse umane

Trattamento dati personali nel rapporto di lavoro

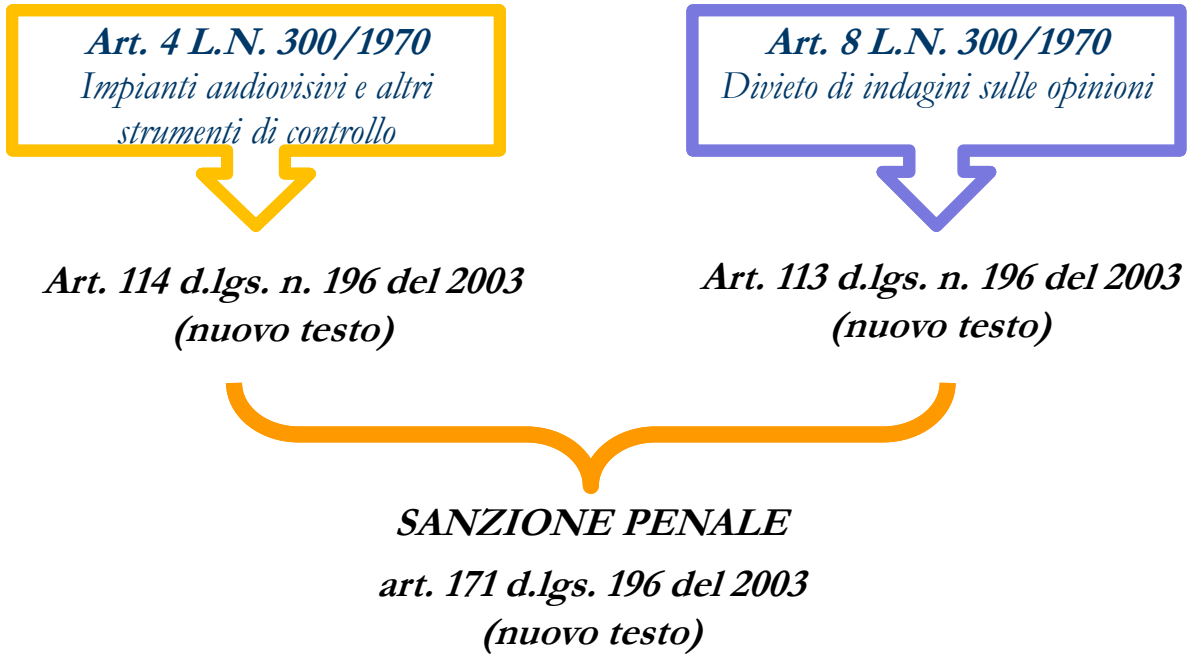
INTERESSATO

la persona fisica cui si riferiscono i dati personali oggetto del trattamento (ad esempio cliente, dipendente)

AUTORIZZATO

Il Titolare del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento dei dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la sua autorità.

Le previsioni nazionali specifiche



Divieto di indagine sulle opinioni

Art. 8 legge n. 300/1970

E' fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

Fase preliminare e/o preassuntiva

QUESTIONARI PREASSUNTIVI

COLLOQUI E/O INTERVISTE

CURRICULUM

SOCIAL

13

Controlli a distanza

Art. 4 l. n. 300/1970 come modificato dall'art. 23 d.lgs. n. 151 del 2015

Impianti audiovisivi ed altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, impiegati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale (primo comma)

SI

Accordo sindacale o autorizzazione amministrativa

Strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e strumenti di registrazione degli accessi e delle presenze (secondo comma)

NO

Accordo sindacale o autorizzazione amministrativa

Controlli a distanza

Art. 4 l. n. 300 del 1970, terzo comma

Le informazioni raccolte ai sensi del primo e secondo comma sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che:

- *Sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli*
- *Sia rispettato quanto disposto dal decreto legislativo n. 196 del 2003*

Controlli con strumenti elettronici

- ✓ *Internet*
- ✓ *Posta elettronica*
- ✓ *Videosorveglianza*
- ✓ *Geolocalizzazione*
- ✓ *Social*

Opinion 2/2017 Gruppo "Articolo 29" dell'8 giugno 2017 sul trattamento dei dati nel posto di lavoro

Art. 4 l. n. 300/1970 come modificato dall'art. 23 d.lgs. n. 151 del 2015

Provvedimento del Garante n. 467 dell'11 ottobre 2018 sulle tipologie di trattamento da sottoporre alla valutazione di impatto

Controlli con strumenti informatici

Adeguata informazione

Regolamento aziendale sull'utilizzo degli strumenti informatici

Gradualità dei controlli

Rispetto dei principi privacy: proporzionalità, necessità, limitazione

Trattamento dati personali nel rapporto di lavoro

Dati particolari (sensibili)

dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale, o all'orientamento sessuale della persona (art. 9, par. 1, Regolamento)

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 (art. 4, n. 15, Regolamento)

Trattamento dati personali nel rapporto di lavoro

Trattamento dati particolari

Demando al Garante di individuare, con Provvedimento di carattere generale, le prescrizioni contenute nelle autorizzazioni generali già adottate, compatibili con il Regolamento e la normativa nazionale ***(art. 21 d.lgs.n.101 del 2018)***

Provvedimento del Garante n. 146 del 5 giugno 2019

Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati

1. Prescrizioni relative al trattamento di categorie particolari di dati nei rapporti di lavoro (aut. Gen. N. 1/2016)

Trattamento dati personali nel rapporto di lavoro

Esempi di categorie di dati particolari

Convinzioni religiose: *fruizione permessi e festività religiose o servizi mensa, ovvero manifestazione, nei casi previsti, dell'obiezione di coscienza*

Opinioni politiche: *permessi o aspettative per incarichi politici o sindacali, trattenute sindacali*

Stato di salute: *invalidità, infermità, gravidanza, puerperio, allattamento, infortuni, esposizioni a fattori di rischio, malattia*

Dati apparentemente neutri

Trattamento dati personali nel rapporto di lavoro

Interessati ai quali i dati si riferiscono

Focus

Candidati

Medico competente

Terzi: Familiari o conviventi dei lavoratori

Trattamento dati personali nel rapporto di lavoro

Trattamenti effettuati nella fase preliminare alle assunzioni

- ✓ *Trattamento delle sole informazioni strettamente pertinenti e limitate a quanto necessario (art. 113 Codice)*
- ✓ *I datori di lavoro devono astenersi dall'utilizzare dati non pertinenti contenuti nei curricula*
- ✓ *Divieto di utilizzo dei dati genetici*

Trattamenti effettuati nel corso del rapporto di lavoro

- ✓ *Convinzioni religiose e/o filosofiche: trattamento esclusivamente per permessi o per erogazione dei servizi mensa;*
- ✓ *Opinioni politiche o appartenenza sindacale: trattamento esclusivamente per permessi, aspettative, esercizio diritti sindacali;*
- ✓ *Divieto trattamento dati genetici*

Trattamento dati personali nel rapporto di lavoro

Prescrizioni relative alle modalità di trattamento

- ✓ *Utilizzo forme di comunicazione, anche elettroniche,* ***individualizzate***
- ✓ *In caso di trasmissione, i documenti devono contenere esclusivamente le informazioni necessarie*
- ✓ *Qualora per ragioni organizzative si mettono a disposizione di terzi i dati relativi alle assenze e presenze dal servizio, non devono essere esplicitate le causali dell'assenza*

Trattamento dati personali nel rapporto di lavoro

Linee guida del Garante novembre 2006

Diagnosi e prognosi non separate

I datori di lavoro sono obbligati, ove possibile, ad adottare misure per prevenire la ricezione della diagnosi, in ogni caso, devono oscurarla

ECCEZIONI

- *Segnalazioni connesse alla tipologia o gravità della malattia*
- *Congedi per eventi e cause particolari*

Trattamento dati personali nel rapporto di lavoro

Linee guida del Garante novembre 2006

E' richiesto il consenso, se non ricorrono le esimenti, per comunicare dati a	
Associazioni	Conoscenti, parenti, familiari

- ✓ *È necessario il consenso per pubblicare informazioni nella intranet aziendale (foto, curricula, etc.)*
- ✓ *Non è richiesto il consenso per le comunicazioni in forma anonima*
- ✓ *Il datore di lavoro deve utilizzare forme di comunicazione individualizzata con il lavoratore*

Trattamento dati personali nel rapporto di lavoro

Linee guida del Garante novembre 2006

Pubblicazione in bacheca o in comunicazioni destinate alla collettività

SI

- ✓ *Ordini di servizio relativi a turni*
- ✓ *Disposizioni riguardanti l'organizzazione del lavoro*
- ✓ *Individuazione mansioni assegnate ai singoli dipendenti*

NO

- X *Emolumenti percepiti o che fanno riferimento a condizioni personali*
- X *Sanzioni disciplinari*
- X *Controversie giudiziarie*
- X *Assenze per malattia*
- X *Iscrizione dei lavoratori ad associazioni*

Trattamento dati personali nel rapporto di lavoro

Dati di carattere giudiziario

- ✓ *Art. 10 Regolamento: il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati*
- ✓ *Art. 2-octies d.lgs. 196/2003: ribadisce la predetta previsione e stabilisce che in mancanza delle disposizioni di legge o di regolamento, il trattamento dei dati in questione e le relative garanzie sono individuati con decreto del Ministro della Giustizia, sentito il Garante, decreto che, allo stato, non è stato ancora emanato.*
- ✓ *Art. 2-octies, 3 comma: il trattamento dei dati personali relativi a condanne penali o a reati o a connesse misure di sicurezza è consentito in alcune ipotesi, tra cui nei casi di "adempimento di obblighi e esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli artt. 9, paragrafo 2, lett. b, e 88 del Regolamento".*

Trattamento dati personali nel rapporto di lavoro

Dati di carattere giudiziario

- ✓ *autorizzazione generale al trattamento dei dati giudiziari da parte di privati, di enti pubblici economici e di soggetti pubblici n. 7/2016, ha cessato di produrre effetti giuridici alla data del 19 settembre 2019.*
- ✓ *allo stato, i datori di lavoro non possono trattare lecitamente dati giudiziari, fatta eccezione per le ipotesi in cui il trattamento degli stessi trovi la sua base giuridica nella legge, come per i casi espressamente previsti dal legislatore per determinate attività*

Trattamento dati personali nel rapporto di lavoro

Dati di carattere giudiziario

- ✓ *Provvedimento Garante n. 247 del 24 giugno 2021: parere sullo schema di decreto del Ministero della Giustizia.*
- ✓ *Modifiche relative ai dati giudiziari in ambito lavoristico:*
- ✓ *a) sopprimere qualsiasi riferimento al consenso del trattamento di questi dati*
- ✓ *b) prevedere che il titolare/datore di lavoro predisponga una valutazione di impatto, al fine di individuare le categorie di personale, o le specifiche posizioni per le quali, in ragione delle mansioni o funzioni svolte, è necessario trattare dati giudiziari ai fini della verifica dei requisiti soggettivi o di onorabilità;*
- ✓ *c) prevedere l'opportunità di sostituire i termini "fissi "di conservazione (stabiliti per un durata pari a due anni dalla cessazione del rapporto, fatta salva l'esigenza di ulteriore conservazione, ai fini di tutela giurisdizionale dei diritti), con un generale richiamo al principio di limitazione della conservazione.*

Agenda

- Presentazione relatore
- Protezione dei dati personali in pratica
- **Bibliografia & sitografia**
- Q&A

Bibliografia & Sitografia

Data breach
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en
https://ec.europa.eu/newsroom/article29/items/612052
https://www.enisa.europa.eu/publications/dbn-severity

Sanzioni:
Sanzione 1)
https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-38FR-2021-sous-forme-anonymisee.pdf
https://www.cybersecurity360.it/legal/privacy-dati-personali/gdpr-azienda-sanzionata-per-inadeguatezza-del-dpo-una-lezione-per-tutti/
Sanzione 2)
https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf
https://www.cybersecurity360.it/legal/privacy-dati-personali/conflitto-di-interessi-del-dpo-maxi-multa-del-garante-belga-a-unazienda/
Sanzione 3)
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043829617?isSuggest=true
Sanzione 4)
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9705632
Sanzione 5)
https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/B64595978C98EFCEC2258606003EC47E/$file/Decision%20F1%20markets%2011.17.00.1.007.263.pdf?openelement
https://www.dataguidance.com/news/cyprus-commissioner-fines-bank-cyprus-%E2%82%AC15000-integrity

Trattamento dati personali nel rapporto di lavoro
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9682603

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1364939

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1417809

Agenda

- Presentazione relatore
- Protezione dei dati personali in pratica
- Bibliografia & sitografia
- Q&A

Agenda

- Presentazione relatore
- Protezione dei dati personali in pratica
- Bibliografia & sitografia
- **Q&A**

Q&A

Contatti

- cesare.desantis@primaedintorni.it
- paola.borghi@uniroma3.it

Grazie...