Cyber Security : Conoscere il fenomeno per ridurne le conseguenze

Milano, Fast, 23 Gennaio 2020

La normativa GDPR in Italia

Ing. Andrea Penza

Data Protection Officer – DPO

Presidente AICT

CEO INTRATEL Srl

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Agenda

- Principi introdotti dal Regolamento (UE) 2016/679
- Regime sanzionatorio
- Designazione e Compiti del DPO
- Privacy by Design
- Privacy by Default
- Privacy, Protezione sei dati e sicurezza informatica e Sicurezza informatica

Principi introdotti dal Regolamento (UE) 2016/679

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Come è noto il **24 maggio 2016** è entrato in vigore il Regolamento (UE) 2016/679.

Il termine ultimo per adeguare le policies aziendali è stato il **25 maggio 2018**.

Il legislatore europeo ha voluto introdurre, tra l'altro, regole più chiare in merito all'informativa ed al consenso stabilendo precisi limiti al trattamento automatizzato dei dati, alla relativa violazione ed all'interscambio degli stessi al di fuori della Comunità Europea.

Chiara la volontà di avere, nel settore, un'unica visione in tutta l'Unione Europea, rendendo chiara e semplice la gestione del proprio dato per ogni cittadino mediante consensi e revoche evidenti.

Art. 4 - oggetto del regolamento:

*«**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*

Art. 4 - gestione:

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

Il consenso ad un certo trattamento, che fino ad oggi poteva anche essere tacito, diventa obbligatoriamente esplicito ed il cittadino potrà verificare in ogni istante come questo viene applicato ed eventualmente revocarlo in modo semplice.

I processi di marketing diretto, le modalità di registrazione e fruizione di servizi internet, la profilazione dell'utente dovranno avere un approccio diverso rispetto a quello finora in essere.

Art. 4:

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

Nel caso di marketing diretto l'interessato avrà sempre diritto di opporsi alle attività di profilazione.

Il modello che permette di trattare correttamente la gestione delle problematiche GDPR nasce da modelli già esistenti e normati; in particolare i legislatori hanno basato la visione del GDPR sulla **ISO 31000** .

Questo standard internazionale tratta in modo preciso il concetto di ***rischio***, che può essere definito come:

“la potenzialità che un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile. La nozione implica che una scelta influenzi il risultato. Le stesse perdite potenziali possono anche essere chiamate "rischi”. Sebbene ogni comportamento umano sia rischioso alcuni hanno una percentuale di rischio maggiore”.

“Per "rischio" possiamo indicare anche la distribuzione dei possibili scostamenti dai risultati attesi per effetto di eventi di incerta manifestazione, interni o esterni ad un sistema.

In questa definizione, il rischio non ha solo un'accezione negativa (downside risk), ma anche una positiva (upside risk).

Esso è definito dal prodotto della frequenza di accadimento e della gravità delle conseguenze (magnitudo)”.

Ogni elemento deve essere quindi misurato dal punto di vista della probabilità di accadimento dei rischi connessi partendo comunque dal principio che, trattandosi di un *rischio possibile*, non si potranno mai realizzare processi atti ad eliminarlo completamente ma solamente a renderne minima la probabilità di accadimento.

Quando non si prenderanno opportune decisioni in merito al trattamento del Rischio, si otterranno NON CONFORMITÀ.

L'intero sistema dovrà essere incentrato sulle politiche di mitigazione del Rischio.

Ovviamente gli strumenti utilizzati per il trattamento del dato personale possono essere anche di carattere tecnologico/informatico; quindi un altro standard diventa basilare per l'approccio al GDPR ed è la **ISO/IEC 27001:2013** (Tecnologia delle informazioni - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti) che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni includendo aspetti relativi alla sicurezza logica, fisica ed organizzativa.

Art. 4

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

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

Regime sanzionatorio

Il sistema sanzionatorio previsto dal GDPR prevede un quadro sanzionatorio unico ed armonizzato in tutti i Paesi UE e soprattutto una responsabilità risarcitoria civile (art. 82) da "*danno da trattamento*"

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

*2. Un **titolare del trattamento** coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un **responsabile del trattamento** risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.*

Il sistema sanzionatorio prevede però la *clausola di esonero da responsabilità* se si dimostra che l'evento dannoso non è in alcun modo imputabile al TdT o al RdT.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

È prevista la **<u>responsabilità in solido</u>**.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Sono previsti **meccanismi di ripartizione della responsabilità risarcitoria** tra titolare (che violi) ed il responsabile (non adempiuto agli obblighi e/o ha agito in modo difforme o contrario).

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

Per ottenere il risarcimento del danno da trattamento bisogna ricorrere all'azione giudiziaria.

All’art. 83 il Regolamento UE 2016/679 prevede che l’autorità di controllo abbia il potere di imporre sanzioni amministrative, a seconda se si tratta di persona fisica o impresa, per un importo pecuniario massimo predeterminato, tenendo conto, nella determinazione del quantum, di determinati indici quali la natura dei dati, la gravità e la durata della violazione, il carattere doloso o colposo della stessa, le misure adottate dal Titolare, la recidività, il nocumento causato, l’adesione a codici di condotta e certificazione.

L’ammontare delle sanzioni amministrative pecuniarie possono arrivare fino ad un massimo di **20 milioni di euro** o fino al **4% del fatturato mondiale totale annuo**.

Designazione del DPO

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Il Regolamento UE 2016/679 prevede per alcune società di adeguare il proprio organigramma privacy inserendo all'interno dello stesso la figura del DPO, acronimo di **Data Protection Officer**.

Negli ordinamenti anglosassoni sono già presenti da anni figure quali *Chief Privacy Officer* (CPO), *Privacy Officer* e *Data Security Officer*.

Il Data Protection Order è una **figura professionale con particolari competenze in campo informatico, giuridico, di valutazione del rischio e di analisi dei processi**, figura può essere rivestita, oltre che da un libero professionista, anche da un dipendente del titolare del trattamento (o del responsabile del trattamento).

L’articolo 38 del GDPR sancisce la posizione di **assoluta indipendenza del DPO**, caratteristica difficile per un dipendente del Titolare o Responsabile del trattamento.

Il DPO non deve trovarsi in alcuna situazione di conflitto di interessi, per evitare facili nomine effettuate per affinità di mansioni pratiche; per esempio non risulterà compliant la nomina a DPO del responsabile ICT.

Analogamente, non potrà essere nominato DPO l’amministratore delegato, il responsabile operativo, il responsabile finanziario o sanitario, il direttore marketing e quello delle risorse umane.

Quindi il DPO:

- **non deve ricevere alcuna istruzione** per quanto riguarda l'esercizio dei compiti preposti;
- deve svolgere la propria attività in modo **del tutto indipendente**;
- deve poter avere la **possibilità di fornire la sua opinione dissenziente** direttamente al vertice gerarchico del Titolare o Responsabile del Trattamento, senza però che il potere decisionale del DPO si estenda oltre i compiti attribuiti di cui all'art. 39 del GDPR;
- **non può essere rimosso** o penalizzato dal Titolare o Responsabile del trattamento nell'adempimento dei propri compiti;
- **non deve essere individuato tra soggetti interni all'organizzazioni che potrebbero determinare un conflitto d'interesse**.

L’articolo 37 del Regolamento UE 2016/679 rende obbligatoria la nomina del DPO quando il trattamento dei dati “*venga effettuato da un’autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali nell’esercizio delle proprie funzioni*”.

Gli “*organismi di diritto pubblico*” sono quegli organismi creati per soddisfare bisogni d’interesse generale a carattere non industriale o commerciale, dotati di personalità giuridica, con una attività finanziata per la maggior parte dallo Stato o da altri organismi di diritto pubblico.

Lo stesso articolo 37 prevede che sussista l'obbligo di nomina del DPO, nel privato, quando il *"**core activities**"* del titolare del trattamento o del responsabile del trattamento *"consista in trattamenti richiedenti il **monitoraggio regolare e sistematico su larga scala**"* nonché quando le attività principali del titolare del trattamento o del responsabile del trattamento *"riguardano il trattamento, su larga scala, di **informazioni sensibili o di dati relativi a condanne penali e a reati**".*

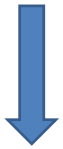
Per **core activities**, attività principali, si intendono le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento.

L'espressione "attività principali" non esclude quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile.

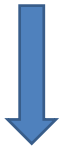
Esempio: l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente.

Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un DPO, come pure le cliniche private, che fanno del trattamento dei dati il proprio *core business*.

Un altro caso riguarda un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche.



L'attività principale dell'impresa consiste nella sorveglianza e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali.



Ne consegue che anche l'impresa in oggetto deve nominare un DPO.

Tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico.

Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali, rendendo quindi facoltativa la nomina del DPO.

Alla domanda circa la definizione di ***larga scala***, si può risponedre: *"non è possibile fornire un numero preciso di dati trattati o di persone interessate necessari a definire la categoria della grande scala"*

Al fine di stabilire se si tratta di un trattamento su larga scala le linee guida del Regolamento consigliano di prendere in considerazione i seguenti elementi:

– il numero di persone interessate ed il volume di dati;

– la durata dell'attività di elaborazione dei dati;

– l'estensione geografica dell'attività di trasformazione degli stessi.

Altri **esempi di trattamento su larga scala** sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di 'geolocalizzazione' raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di

- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Mentre, **esempi di trattamento non su larga scala** sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Monitoraggio regolare e sistematico degli interessati è un concetto che non trova definizione all'interno del GDPR; tuttavia, il **Considerando 24** menziona il "*monitoraggio del comportamento di detti interessati*" ricomprendendovi tutte le forme di tracciamento e profilazione su Internet, anche per finalità di pubblicità comportamentale.

La nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online e il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.

Con “*regolare*” si intende uno dei seguenti significati:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

Mentre con “*sistematico*” si intende uno dei seguenti significati:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell’ambito di un progetto complessivo di raccolta di dati;
- svolto nell’ambito di una strategia.

Esempi di *monitoraggio regolare e sistematico*:

- curare il funzionamento di una rete di telecomunicazioni;
- prestazione di servizi di telecomunicazioni;
- reindirizzamento di messaggi di posta elettronica;
- attività di marketing basate sull'analisi dei dati raccolti;
- profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio);
- tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili;

- programmi di fidelizzazione;
- pubblicità comportamentale;
- monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili;
- utilizzo di telecamere a circuito chiuso;
- dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

Si raccomanda a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un DPO, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.

Tale analisi fa parte della documentazione da presentare, su richiesta, all'Autorità Garante per la protezione dei dati, in caso di verifiche, controlli ed ispezioni.

Compiti del DPO

L'articolo 39 del Regolamento UE 2016/679 elenca i principali compiti del Data Protection Officer che sono:

- fornire consulenza e informare il Titolare o il Responsabile del Trattamento e tutti coloro che effettuano il trattamento in merito agli obblighi derivanti dal Regolamento;
- sorvegliare che le disposizioni in merito alle attività di controllo vengano rispettate;
- fornire pareri sulla valutazione d'impatto sulla protezione dei dati sorvegliandone il corretto svolgimento (di cui l'art. 35);
- collaborare con le autorità di controllo e fungere da punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva (di cui l'art. 36)

Il principale compito del DPO è il controllo del rispetto del GDPR, raccogliendo dati, analizzando la compliance, informando, consigliando e formulando raccomandazioni al Titolare o al Responsabile.

Il WP29 chiarisce: "*Il controllo della conformità non significa che sia il DPO ad essere personalmente responsabile nel caso in cui vi sia una non conformità.* ***Il GDPR rende chiaro che è il Titolare, non il DPO, ad essere tenuto all'attuazione di misure tecniche e organizzative che garantiscano e che dimostrino che il trattamento viene eseguito in conformità al GDPR***".

Privacy by Design

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Il concetto di *privacy by design* risale al 2010, già presente negli Usa e Canada e poi adottato nel corso della 32ma Conferenza mondiale dei Garanti privacy; la definizione fu coniata da Ann Cavoukian, Privacy Commissioner dell'Ontario (Canada).

I principi che reggono il sistema sono i seguenti:

- **prevenire non correggere**, cioè i problemi vanno valutati nella fase di progettazione;
- privacy come impostazione di default;
- privacy incorporata nel progetto;

- massima funzionalità, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- sicurezza durante tutto il ciclo del prodotto o servizio;
- **trasparenza**;
- centralità dell'utente.

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Quindi, il sistema di tutela dei dati personali deve porre l'utente al centro, in tal modo obbligando ad una **tutela effettiva da un punto sostanziale, non solo formale**.

Non è sufficiente che la progettazione dei sistema sia conforme alla norma se poi l'utente non è tutelato.

L'approccio GDPR è basato sulla valutazione del rischio (*risk based approach*), definito tramite i Considerando 75 e 76, con il quale si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

L'obbligo di *privacy by design* è basato sulla valutazione del rischio, così come altri obblighi (es. notifica ai Garanti nazionali), per cui le aziende devono valutare il rischio inerente alle loro attività.

Tale valutazione va fatta al momento della progettazione del sistema, quindi prima che il trattamento inizi.

Chiaramente si deve tenere conto anche del tipo di dati trattati, per cui in presenza di un trattamento che coinvolge dati di minori gli obblighi dovranno essere più stringenti, in considerazione del fatto che il rischio è maggiore.

L'approccio basato sul rischio comporta che si deve tenere conto dello stato della tecnologia, per cui **il trattamento va adattato nel corso del tempo**.

Un esempio che può aiutare a capirne la complessità riguarda i processi deputati alla gestione del ciclo di vita delle applicazioni che trattano dati personali: per essere conformi al principio della *privacy by design* occorre integrarli, quantomeno, con le attività di:

- identificazione del flusso dei dati personali e dei trattamenti a cui saranno sottoposti durante tutto il loro ciclo di vita all'interno dell'organizzazione;
- identificazione puntuale dei requisiti di sicurezza che le applicazioni e l'infrastruttura tecnologica a supporto devono soddisfare per tutelare la RID dei dati personali, in qualunque stato essi si trovino (in use, in motion, at rest);
- definizione degli standard di programmazione che consentano di implementare applicazioni esenti da vulnerabilità dovute a tecniche di programmazione non sicure;

- definizione degli standard architetturali necessari a soddisfare i requisiti di sicurezza definiti;
- definizione delle tecniche di mascheramento (o similari) dei dati personali qualora se ne preveda l'utilizzo in ambienti diversi da quello di produzione (test, formazione, …);
- integrazione dei piani di test con le attività di verifica della corretta implementazione dei requisiti di sicurezza definiti, sia a livello applicativo che infrastrutturale;
- prevedere delle attività di test volte a verificare l'efficacia delle misure di sicurezza e degli standard applicativi e architetturali implementati (ethical hacking, penetration test, vulnerability assessment, code review, …).

Tutte le principali funzioni aziendali (Information Security, Risk Management, ICT, Legal, Compliance, Organizzazione, HR, Internal Audit,…), dovranno dare il loro contributo, **con il supporto ed il coordinamento del DPO**, alla revisione ed integrazione, per quanto di loro competenza, dei processi e delle tecnologie in uso al fine di **implementare un modello di Privacy by Design definito e condiviso e di garantirne l'efficacia nel tempo**.

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Privacy by Default

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Il principio di ***privacy by default*** stabilisce che il titolare debba attuare specifiche misure che garantiscano un idoneo trattamento dei dati, personalizzato, a seconda delle finalità e del tipo di operazioni da porre in essere.

Tale obbligo varia a seconda della quantità dei dati personali raccolti, della portata del trattamento nonché del periodo di conservazione e dell'accessibilità.

Il responsabile del trattamento deve garantire che siano **trattati di default solo i dati personali necessari per ciascuna finalità specifica del trattamento** e che, in particolare, **la quantità dei dati raccolti e la durata della loro conservazione non devono andare oltre il minimo necessario per le finalità perseguite**.

La **minimizzazione** costituisce una misura di riduzione del trattamento by default finalizzata a impostare a priori la **massima protezione dei dati attraverso il loro minimo trattamento**, sia in fase di raccolta sia in fase di trattamento successivo all'acquisizione dei dati personali, secondo i principi di necessità, pertinenza, adeguatezza e non eccedenza rispetto alle finalità.

Detti meccanismi garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone e che gli interessati siano in grado di controllare la distribuzione dei propri dati personali.

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

La privacy by default comporta, da una parte, che in un complessivo approccio di progettazione di sistemi informatici funzionale alla tutela della privacy, determinate informazioni debbano essere protette in modo rafforzato.

Dall'altra parte comporta l'utilizzo di determinate impostazioni in automatico di maggiore tutela per l'utente.

Tali impostazioni sono scelte da chi costruisce il sistema informatico con la possibilità di cambiamento da parte dell'utente dell'opzione prescelta.

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Privacy e Sicurezza informatica

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Privacy e sicurezza informatica

- *Vulnerabilità*
- *Minacce e misure di sicurezza*

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Vulnerabilità

Misure di sicurezza

Cosa devono garantire le misure di sicurezza

Riservatezza dei dati

I dati devono poter essere trattati solo dal personale autorizzato

Integrità dei dati

I dati devono poter essere modificati solo da chi è espressamente autorizzato

Disponibilità dei dati

I dati, quando servono, devono essere sempre accessibili

Misure di sicurezza

Da cosa devono essere protetti i dati ed in generale le informazioni

Guasti Hardware - possono essere distinti in:

guasti che impediscono temporaneamente la disponibilità dei dati quali ad esempio, la mancata accensione di un server/pc per problemi su scheda madre del sistema o su alimentatore

guasti che altre alla indisponibilità dei dati possono provocare la perdita dei dati stessi,come ad esempio può succedere in caso di un guasto ad un Hard Disk

Errore Software

si tratta dei cosiddetti bug software che impediscono il corretto funzionamento del software

Attacco informatico

virus, hackeraggio, ecc.

Misure di sicurezza

Errore umano

ad esempio cancellazioni di file, errata configurazione di software e protocolli, ecc.

Furto

furto di un computer portatile, di un server ma anche di soli file qualora si lascino i computer incustoditi con le sessioni di lavoro aperte

Evento naturale o incidenti

Incendi, alluvioni, terremoti, allagamenti, cortocircuiti, ecc.

Differenza tra Vulnerabilità e Minacce

Un minaccia è di solito:

- una persona che **può attaccare** un bene o una risorsa con uno scopo preciso in mente
- Un cosa (un fiume che esonda, un cortocircuito, un incendio, ecc.)

Una vulnerabilità **è una debolezza del sistema** o la mancanza di misure di sicurezza che possono essere sfruttate da persone o cose

- Un esempio di vulnerabilità potrebbe essere un argine di un fiume danneggiato, che qualora il fiume lasciasse il suo letto, potrebbe facilmente cedere
- un altra vulnerabilità potrebbe essere lasciare acceso un computer consentendo a persone non autorizzate di accedere ai dati

Vulnerabilità e Minacce

- Le minacce (i rischi) e quindi anche le vulnerabilità possono essere normalmente legate ai seguenti tre ambiti:
  - Comportamento degli operatori: disattenzione, incuria, atti dolosi, ecc.
  - Strumenti di lavoro: computer, archivi informatici e cartacei, ecc.
  - Contesto in cui opera l'azienda: posizione geografica, struttura degli edifici in cui opera, tipologia di impianti installati, ecc.

Vulnerabilità

- Possibili vulnerabilità legate al comportamento degli operatori:
  - Lasciare della postazione di lavoro senza effettuare la disconnessione
  - Lasciare gli archivi cartacei incustoditi
  - Insufficiente formazione sulla gestione dei dati personali
  - Gestione scorretta delle credenziali di accesso
  - Uso scorretto degli strumenti di lavoro

Vulnerabilità

- Possibili vulnerabilità legate agli strumenti di lavoro:
  - Mancanza di antivirus
  - Utilizzo di software non aggiornato
  - Mancanza di Firewall
  - Software complesso da utilizzare
  - Assenza o inadeguatezza delle copie di backup
  - Mancanza di procedure di accesso con credenziali

Vulnerabilità

- Possibili vulnerabilità legate al contesto in cui opera l'azienda:
  - Mancata sorveglianza delle aree protette
  - Mancanza di procedure di registrazione degli accessi
  - Mancanza di procedure di registrazione di entrata/uscita documenti
  - Mancanza di serrature di sicurezza
  - Assenza di sistemi di antincendio
  - Assenza piani di emergenza
  - Manutenzione impianti inadeguata

Minacce e misure di Sicurezza e Protezione

Minacce e Misure di Sicurezza e Protezione

- Le minacce e le misure di protezione per la protezione dati personali sono un sottoinsieme delle minacce che gravano su una organizzazione e tutte possono essere trattate all'interno del trattamento dei rischi aziendali
- Di seguito ci si concentrerà sulle minacce inerenti la protezione dati personali o gli ambiti e ambienti, anche fisici, che possono avere rilevanza sulla protezione dati personali

Minacce e Misure di Sicurezza e Protezione

- Il miglior modo di individuare minacce passa attraverso la condivisione della tematica e il confronto con le risorse coinvolte per analizzare la loro visione e la loro sensibilità alla minaccia
- L'analisi e l'annotazione delle singole minacce, prendendole tutte in esame ed annotando su ciascuna i possibili riscontri sull'ambito analizzato permette di dare una visione il più completa possibile e migliora l'accountability del Titolare del Trattamento

Minacce e Misure di Sicurezza e Protezione

- Possibili minacce legate al comportamento degli operatori:
  - Sottrazione credenziali di autenticazione
  - Disattenzione o incuria
  - Errori materiali nello svolgimento delle mansioni
  - Errori materiali nell'utilizzo dei software
  - Ignoranza delle procedure di gestione dei dati
  - Alterazione volontaria dei dati

- Trattamento illecito dei dati
- Comunicazione illegale dei dati
- Falsificazione dei diritti di accesso

Minacce e Misure di Sicurezza e Protezione

- Possibili minacce legate agli strumenti di lavoro:
  - Attacchi di virus informatici
  - Spamming e hackeraggio
  - Malfunzionamento software
  - Accessi non autorizzati
  - Intercettazione dei dati
  - Degrado o blocco del sistema informatico

  - Guasto delle apparecchiature
  - Corruzione dei dati

Minacce e Misure di Sicurezza e Protezione

- Possibili minacce legate al contesto in cui opera l'azienda:
  - Accesso non autorizzato a locali ad accesso ristretto
  - Sottrazione di documentazione
  - Eventi distruttivi naturali (alluvione, terremoto, ecc.)
  - Eventi distruttivi artificiali (incendio, allagamento, cortocircuito, ecc.)
  - Guasti ad impianti
  - Errori di gestione della sicurezza fisica

- Radiazioni elettromagnetiche
- Mancata manutenzione del sistema informatico
- Mancata manutenzione degli impianti e dei mac
- Furto

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazio

Minacce e Misure di Sicurezza e Protezione

- La risposta alle minacce può essere una prevenzione o una protezione
  - La prevenzione interviene sulla probabilità di accadimento di una minaccia
  - La protezione interviene sul danno che la minaccia può generare modificandolo

Minacce e Misure di Sicurezza e Protezione

- Poiché la trattazione dei dati avviene spesso per via informatica buona parte delle misure tecniche di sicurezza sono interventi informatici e assume particolare importanza l'approccio alle protezioni:
- PROTEZIONI ATTIVE:
  - Definizione di regole tecniche; antivirus; antispam; firewall; crittografia anche di apparati mobili; tracciamento delle attività degli operatori (log); controlli degli accessi; crittografia delle password, profilo di accesso ai dati, navigazione protetta, ….

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

- PROTEZIONI PROATTIVE:
  - Definizione di regole organizzative, formazione, informazione, ridotta disponibilità di dati (minimizzazione), aggiornamento del personale, …

Minacce e Misure di Sicurezza e Protezione

- Altre misure tecniche di protezione sono:
  - gruppi di continuità
  - sistemi antincendio
  - centrale di allarme
  - sorveglianza e telesorveglianza
  - armadi blindati

  - sistemi di controllo fisico degli accessi
  - sistemi di distruzione documenti
  - ed anche sistemi di climatizzazione a protezione delle sale serv.

Minacce e Misure di Sicurezza e Protezione

- La risposta ad una minaccia può coinvolgere:
  - Le tecnologie impiegate
  - Le scelte «applicative» adeguate relative ai dati
  - La consapevolezza di tutte le entità coinvolte in operazioni di trattamento

- La risposta o l'insieme di esse viene definito Misure di Sicurezza e Protezione. E' necessario che ad ogni minaccia prevista sia definita una o più misure di sicurezza che rispondano alla minaccia. Il processo di analisi passa dalle stesse modalità di gestione del rischio

Minacce e Misure di Sicurezza e Protezione

- Le misure di sicurezza possono essere di tipo organizzativo, procedurale, tecnico
  - Le organizzative implicano la scelta di ridondanze o di divisioni delle risorse impiegate nell'attività
  - Le procedurali implicano la definizione di precisi passi e suddivisione di responsabilità per dare evidenza di passaggi di controllo effettuati
  - Le tecniche implicano l'inserimento nel processo di sistemi hardware e/o software di protezione

Minacce e Misure di Sicurezza e Protezione

- L'attribuzione di responsabilità a persone diverse per effettuare controlli da punti di vista diversi ed in momenti diversi può essere una misura organizzativa

- La formazione del personale e la diffusione continua di cultura rientra fra le misure organizzative di risposta alle minacce

Minacce e Misure di Sicurezza e Protezione

- La presenza di una politica per la protezione dati dichiarata dall'organizzazione può rappresentare un primo embrione di misure di sicurezza
- Altre misure di sicurezza organizzativa sono:
  - La presenza di procedure operative precise che dettagliano i passi operativi del processo può ridurre i rischi di errori o di manomissione di dati personali da parte degli operatori

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

  - La presenza di regolamenti disciplinari che disciplinino eventuali sanzioni in caso di errore o di manomissioni per mancata attenzione

INtraTEL s.r.l. Idee . Servizi . Soluzioni

Protezione dei dati e Sicurezza informatica

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Protezione dei Dati e Sicurezza informatica

- *Tecniche di Backup*
- *Disaster Recovery*

Cosa garantisce la sicurezza informatica

Riservatezza dei dati

I dati devono poter essere trattati solo dal personale autorizzato

Integrità dei dati

I dati devono poter essere modificati solo da chi è espressamente autorizzato

Disponibilità dei dati

I dati, quando servono, devono essere sempre accessibili

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Quanto si ha bisogno dei dati backup

Anche in ambito protezione dei dati personali **prevenire è meglio che curare**, ma quando le tecniche di prevenzione falliscono allora scatta il piano di Disaster Recovery per ripristinare la disponibilità dei dati a partire dalle copie di backup

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Tecniche di sicurezza informatica

La sicurezza informatica su basa su **due tipologie di tecniche**

Tecniche di Prevenzione

Adozione di misure **tecniche ed organizzative adeguate**, quali ad esempio: sistemi hardware ridondati, policy sull'utilizzo degli strumenti informatici, strumenti per proteggersi da attacchi informatici (antivirus, firewall), formazione, backup dei dati, criptaggio, ecc.

Tecniche di Reazione (Ripristino Backup)

Qualora le tecniche di prevenzione falliscono si dovrà ricorrere al ripristino dei dati di backup attivando il piano di disaster recovery

Minacce da cui proteggere i dati

Guasti Hardware del sistema informatico

- guasti che impediscono temporaneamente la disponibilità dei dati quali ad esempio, la mancata accensione di un computer
- guasti che oltre alla indisponibilità dei dati possono provocare la perdita dei dati stessi, ad es. succede in caso di un guasto ad un Hard Disk

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

Errori dei Software

- si tratta dei cosiddetti bug che impediscono il corretto funzionamento del software

Attacchi informatico

- virus, hackeraggio, ecc.

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Minacce da cui proteggere i dati

Errori del personale autorizzato

ad esempio cancellazioni di file, errata configurazione di software e protocolli, ecc.

Furto

furto di un computer portatile, di un server ma anche di soli file qualora si lascino i computer incustoditi con le sessioni di lavoro aperte

Eventi naturali ed incidenti

Incendi, alluvioni, terremoti, ecc.

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Le regole per un backup efficace - I

- Definire l'intervallo di backup, ovvero ogni quanto tempo si fa il backup (Recovery Point Objective o RPO)
- Definire i tempi di ripristino, ovvero tempi necessario per ripristinare i dati (Recovery Time Objective o RTO)
- Definire la tipologia di backup da adottare: completo, differenziale, incrementale
- Definire la granularità del ripristino, ovvero possibilità di poter ripristinare in caso di necessità anche un singolo file/singola mail, andato/a perso

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Le regole per un backup efficace - 2

Prevedere di avere più copie di backup e non una sola copia

Fare delle prove di ripristino dei dati di backup

Questo è uno specifico requisito del regolamento europeo e deve essere previsto nel piano di disaster recovery

Attenzione a proteggere i dati di backup dagli attacchi da virus di tipo ransomware

Strategie di Backup - I

Individuazione dei dati per i quali è necessario eseguire il backup. Si dovrà distinguere tra i dati statici e dati dinamici:

- i dati statici sono quelli che non cambiano o cambiano soltanto di rado (es. sistemi operativi, software applicativi, dati anni precedenti)

- i dati dinamici invece sono quelli che sono prodotti in continuazione: analisi, esami clinici, cartella clinica, ecc.

I dati statici necessitano di backup meno frequenti rispetto ai dati dinamici; in teoria, è sufficiente eseguire una o più copie una volta e conservarle in un luogo lontano da quello di lavoro, per garantirsi la possibilità di ripristino in caso di disastro

Strategie di Backup - 2

I **dati dinamici** necessitano di un backup ogni qualvolta i dati stessi cambiano; solo così si avrà sempre la garanzia di poter ripristinare tutto il lavoro, al limite perdendo quello di una sola giornata. Se la modifica dei dati è molto rapida, si può optare per la creazione di più di un backup al giorno, operazione che però diventa molto pesante e complessa ma che in ambito sanitario è auspicabile

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

STRATEGY

Progettazione del Backup: RTO e RPO

- L'intervallo con cui si effettua il backup porta a definire uno dei parametri di cui tener conto nel momento in cui si progetta una soluzione di backup. Tale parametro è il cosiddetto **Recovery Point Objective (RPO)** e disciplina quanti dati l'azienda è disposta a perdere. Ad esempio se si è disposti a perdere i dati di un giorno allora sarà necessario eseguire delle copie di backup giornaliere
- L'altro parametro è il **Recovery Time Objective.** Esso definisce quanto tempo l'azienda può operare a seguito di un evento che ha compromesso l'integrità e la disponibilità dei dati
- Sia l'**RTO** che l'**RPO** sono normalmente espressi in ore o minuti. Tanto più bassi sono i valori tanto più complessa e costosa sarà la soluzione di backup da adottare

Progettazione del Backup: RTO e RPO a zero

- Qualora per esigenze organizzative si ha la necessità di essere operativi 24 ore al giorno (H24) allora si ha il caso limite di avere RTO e RPO a zero
  - In questo caso è necessario implementare una infrastruttura ICT che garantisca una ridondanza dei dati sia in termini di copie degli stessi, (ovvero ridondanza di hw, software, database) sia in termini di posizione geografica (ridondanza spaziale)

Progettazione del Backup: backup retantion

Un altro importante parametro di cui tener conto nel progettare una soluzione di backup è la **retention**, ovvero il tempo di conservazione dei dati salvati: il numero minimo di copie del backup che vogliamo che siano tenute online e per quanti giorni

Ad esempio nel caso di backup giornaliero, una retention di 7 giorni si traduce praticamente nel fatto che vengono conservati una copia di backup per ogni giorno della settimana per cui in caso di necessità è possibile tornare indietro a recuperare file di una settimana prima.

Progettazione del Backup: modalità di backup

Il backup può essere eseguito in tre differenti modalità: completo, incrementale, differenziale

Backup Completo: ogni volta che si effettua il backup si copiano tutti i file anche quelli non modificati dal backup precedente

Backup Differenziale: La prima volta si fa il backup completo e poi ogni volta si fa il backup di ciò che è cambiato rispetto al backup completo; ciò implica che più passa il tempo dal backup completo e più i differenziali aumentano di volume

Backup Incrementale: La prima volta si fa il backup completo e poi ogni backup incrementale fa il backup di ciò che è cambiato rispetto all'ultimo backup fatto (incrementale o completo) e non rispetto all'ultimo completo

Relazione tra le minacce e il backup dei dati - I

Guasti Hardware

In generale, in caso di guasto hardware è sufficiente avere l'ultima copia dei dati e fare il ripristino dei stessi

Errore Software

In generale, anche in caso di guasto software è sufficiente avere una l'ultima copia dei dati e fare il ripristino dei stessi

Attacco informatico

In caso di attacco informatico è importante la **retention** in quanto, in caso di attacco da parte di virus di tipo ransomware c'è il rischio di accorgersi dell'attacco dopo che si è proceduto a fare una copia di backup. Avere la possibilità di tornare indietro nel tempo con le diverse copie di backup a disposizione ci tutela da questa tipologia di attacco

Relazione tra le minacce e il backup dei dati - 2

Errore umano

In generale, anche in caso di errore umano è importante la **retention** in quanto, ci si potrebbe accorgere dell'errore solo dopo aver effettuato la copia backup. Avere la possibilità di tornare indietro con i backup a disposizione ci tutela da questa minaccia

Furto

In questo caso è importante, anzi indispensabile avere la/le copia/e di backup in luoghi protetti o in una sede diversa

Evento naturale

Per proteggersi da eventi naturali (es. terremoto) è necessario avere il backup in un luogo diverso che si trovi a centinaia di km di distanza dal luogo che ospita i dati in produzione

Dove si conservano i backup

Backup locale in cassaforte ignifuga

Backup remoto in Cloud Computing

I dati vengono conservati in Data Center protetti e controllati che garantiscono anche la protezione dagli eventi naturali in quanto i dati sono conservati in remoto

Nel caso si utilizzi il Cloud Computing bisogna prestare **particolare attenzione** a DOVE vendono conservati i dati per non infrangere il Regolamento

Piano di Disaster Recovery - I

Per **Disaster Recovery**, in informatica ed in particolare nell'ambito della sicurezza informatica, si intende l'insieme delle misure tecnologiche e organizzative atte a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione dei servizi a fronte di gravi emergenze che ne intacchino la regolare attività

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Piano di Disaster Recovery - 2

Progettare una soluzione di backup efficace è solo una della componenti necessarie per realizzare un piano di disaster recovery. Le altre principali componenti sono:

- Definire le risorse umane che dovranno attuare, in caso di necessità, il piano di disaster recovery
- Definire processi e procedure legate al piano di disaster recovery
- Eseguire periodicamente delle prove di attuazione del piano di disaster recovery

INtraTEL s.r.
Idee . Servizi . Soluzio

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni

Conclusione

Grazie per l'attenzione!!!!

andrea.penza@intratel.it
andrea.penza@societyaict.it

INtraTEL s.r.l.
Idee . Servizi . Soluzioni

AICT Society AEIT per la Tecnologia dell'Informazione e delle Comunicazioni