Responsabilità e Consapevolezza nel mondo digitale

unione
segretari comunali
ticinesi

Dr.- Ing.- Alessandro Trivilini, Ph.D.

www.trivilini.info

10 settembre 2021

Definizione di dato personale
CH - UE

Definizione di dato personale EU

GDPR (EU 2016/679, General Data Protection Regulation)

https://gdpr.eu/

Regolamentazione europea sulla trattazione del dato personale

Definizione di «**dato personale**»

"(...) qualsiasi informazione riguardante una persona fisica identificata o identificabile. Una persona fisica è identificabile o identificata, direttamente o indirettamente, con un 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]

Definizione di dato personale CH

25 settembre 2020

Approvazione da parte del Parlamento svizzero della revisione totale della legge federale sulla protezione dei dati (LPD).

Dato personale

Allineamento alla definizione proposta e in essere dalla GDPR europea.

«*(..) tutte le informazioni che si riferiscono a una persona identificata o identificabile.*»

Per esempio: informazioni sulla salute, razza, etnia, religione, opinion, attività politiche o sindacali, informazioni sull'assistenza sociale, perseguimenti e sanzioni amministrative e penali, dati biometrici che I dentificano una persona in modo univoco

Quali sono per definizione?

- **Informazioni biografiche o situazioni di vita attuale**: data di nascita, numero AVS, numero di telefono, indirizzo email, IP fisso.
- **Aspetto fisico e comportamento**: colore degli occhi, peso e tratti del carattere.
- **Dati relativi al posto di lavoro e sull'istruzione**: salario, informazioni fiscali, numero di matricola dello studente, voti e giudizi personali.
- **Dati privati e soggettivi**: religione, opinioni politiche e dati di geolocalizzazione.
- **Salute, malattia e dati genetici**: anamnesi, congedi per malattia.

I diritti fondamentali

In Svizzera, la nuova legge sulla protezione dei dati tutela la personalità e i diritti fondamentali delle persone fisiche.

Per esempio, i diritti fondamentali sono il diritto alla vita, il diritto al matrimonio e alla famiglia, il diritto d'informazione e i **diritti della personalità.**

Il diritto al nome, il diritto all'onore, il diritto alla reputazione e **il diritto alla riservatezza.**

Due diritti da conoscere

Il **diritto alla riservatezza** è tutelato dalla nuova legge sulla protezione dei dati.

Ogni persona ha il diritto di consultare ogni raccolta dei suoi dati personali fatta, per esempio, da un'azienda proprietaria di una piattaforma didattica, con la possibilità di richiederne l'eliminazione se la ritiene sbagliata.

Il diritto all'autodeterminazione informativa indica che che ogni persona ha il diritto di poter scegliere a chi comunicare i suoi dati personali e sapere a priori in che modo verrano comunicati, con quale scopo, strumento e da chi verranno utilizzati.

Due principi da conoscere

Il principio di minimizzazione impone a chi tratta i dati personali di farlo utilizzando il numero **minimo** di dati che gli permetta di raggiungere il suo obiettivo di elaborazione.

Chi chiede i dati personali deve tenere conto che c'è un limite.

Il principio di finalità indica che i dati personali **non** possono essere elaborati per uno scopo incompatibile con quello per il quale sono stati raccolti.

Tutela il fatto che i dati personali non possono essere usati a tua insaputa per uno scopo diverso da quello che ti hanno comunicato al momento della richiesta.

Il trattamento dei dati e il consenso

Con il termine **trattamento** si intende qualsiasi operazione effettuata sui dati, come per esempio la raccolta dei dati, l'elaborazione, la diffusione, la pubblicazione, la trasmissione, la memorizzazione, l'archiviazione o l'eliminazione dei dati.

Il trattamento dei dati personali è subordinato al **consenso** della persona interessata.

Il consenso è valido solo se espresso liberamente e dopo aver informato adeguatamente la persona sull'uso che verrà fatto dei suoi dati personali.

Chi raccoglie i dati personali deve anche mettere a disposizione in modo trasparente e ben visibile l'opzione di rimozione del consenso, in gergo tecnico chiamata "**opt-out**".

Principi del trattamento

Art. 6/7 revLPD

Legittimità

I dati personali possono essere trattati solo in modo lecito.

Buona fede e proporzionalità

È possibile trattare solo i dati idonei e necessari per le finalità del trattamento (rapporto adeguato tra scopo e mezzi).

Sicurezza

Provvedimenti tecnici e organizzativi appropriati per garantire che la sicurezza dei dati personali sia adeguata al rischio

Durata della conservazione

I dati personali devo essere distrutti o resi aninimi appena non sono più necessari per lo scopo del trattamento.

Trasperanza

La raccolta dei dati personali e in particolare lo scopo del loro trattamento devono essere riconoscibili per la persona interessata.

Prinicipio di sicurezza non più trascurabile

Tra i principi di sicurezza indicata dal framework indicati come vincolanti, ai fini di una corretta messa in sicurezza dei dati sensibili e delle infrastrutture critiche, emerge la seguente:

Organizzazione e responsabilità

Per garantire la sicurezza, l'organismo o l'impresa devono creare una struttura generale che stabilisca chiaramente compiti, responsabilità e competenze. In questo contesto va inoltre definita e applicata la cosiddetta strategia defense-in-depth. I rischi TIC devono essere inseriti in una strategia ***globale di gestione dei rischi****; condizione, questa, per individuare possibili minacce e mettere a punto le rispettive misure (...)*

https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html

La sicurezza informatica

Il Centro Nazionale per la Sicurezza Informatica - NCSC

www.ncsc.admin.ch

Gestione della sicurezza informatica per pubbliche amministrazioni e aziende con medesime line guida condivise CH – EU

L’approccio al NIST

Stato dell’arte della cyber sec in CH

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Strategia nazionale per la protezione della Svizzera contro i rischi cibernetici (SNPC)

Il Consiglio federale intende combattere attivamente i cyber-rischi e adottare le misure necessarie per preservare la sicurezza della Svizzera contro le minacce provenienti dal cyberspazio. A questo scopo ha licenziato la nuova SNPC per il periodo 2018–2022.

La Strategia comprende lo sviluppo di competenze e conoscenze, la promozione della cooperazione internazionale e dei provvedimenti di cyber difesa adottati per rafforzare la gestione degli incidenti e delle crisi, come pure la collaborazione nel perseguimento penale dei cyber-reati (…).

Detection&Response

Strategia SNPC 2018-2022

► Scarica il documento:
www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/ncs_strategie.html

Luglio 2020
Nuovo National Cyber Securtiy Center (NCSC) - www.ncsc.admin.ch

Lo standard TIC

Tecnologie dell'Informazione e della Comunicazione

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Protezione dai cyber-rischi: la Confederazione sostiene le aziende in Svizzera

Per tutelare i gestori dai cyber-rischi, che costituiscono una minaccia crescente per questi servizi, l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha elaborato uno standard minimo, presentato il 27 agosto 2018.

L' Ufficio federale per l'approvvigionamento economico del Paese (UFAE) ha analizzato la vulnerabilità ai cyber-rischi in svariati rami d'importanza vitale. Sono stati esaminati l'approvvigionamento di elettricità, acqua potabile e derrate alimentari, ma anche i trasporti su gomma e ferrovia. In base ai risultati **l'UFAE ha elaborato uno standard minimo per rafforzare la resilienza informatica.**

Lo standard minimo per **rafforzare** la resilienza informatica comprende diverse funzioni (identificare, proteggere, intercettare, reagire e ripristinare) e offre agli utenti **106** istruzioni concrete per migliorare la resilienza informatica ai cyber-rischi. I provvedimenti proposti sono di natura organizzativa o tecnica, tra cui prescrizioni per stilare un inventario completo dell'hardware e del software, formare e addestrare i collaboratori, garantire la protezione dei dati, individuare con anticipo le minacce ecc.

Dr.- Ing.- Alessandro Trivilini, Ph.D.

Lo standard TIC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Tecnologie dell'Informazione e della Comunicazione

Lo standard in breve:

- La prima parte contiene informazioni pratiche sulla resilienza informatica e funge da guida di riferimento.
- Il framework offre agli utenti una ricca gamma di provvedimenti, suddivisi in cinque tematiche: identificare, proteggere, intercettare, reagire e ripristinare.
- Il tool di valutazione permette alle aziende di misurare il proprio grado di resilienza informatica, o di farlo verificare da società esterne (audit). **Il tuo posizionamento rispetto ai punti minimali.**

Le 5 fasi del NIST

► **Scarica il documento ufficiale:**
https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-71944.html

► **Fai il test. Norme minimale TIC - Outil d'évaluation (XLS, 3 MB, 27.08.2018):**
https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-71944.html

Il triage per gestire i rischi cyber «by design»

Security governance & compliance

- GDPR e LPD
- ISO 27001 (security management)
- NIST (Cyber securtiy framework US, detection and response)
- ISO 22301 (business continuity)
- ISO 27037 (digital forensics)

Security audit

- Penetration tests
- Assessment sulle vunerabilità
- Test di ingegneria sociale
- Incident response (IRP)
- Digital forensics

Cyber Education

- Approccio intedisciplinare alla formazione continua

Le 5 fasi del NIST

Prepararsi a incidente informatico

Fasi di un cyber attacco e contromisure

Macro fasi utili per la creazione di un piano di risposta agli incidenti informatici

Fase	Contromisure
1. Reiconoscimento • Identificazione dell'obiettivo • Ricerca delle vulnerabilità	• Monitoraggio e logging • Consapevolezza della situazione • Collaborazione
2. Attacco sull'obbiettivo • Identificazione delle vulnerabilità • Abbattimento dei controlli restanti	• Progettazione di sistemi strutturali • Controlli standard (per esempio ISO 27001) • Penetration test
3. Raggiungimento degli obiettivi • Interruzione dei sistemi • Estrazione dei dati • Manipolazione delle informazioni	• Pianificazione della risposta agli incidenti di cyber sicurezza • Piani di continuità aziendale e ripristino • Assicurazione per la cyber sicurezza

Come prepararsi a un incidente informatico?

«*Ho fatto tutto ciò che era plausibile fare per …*

- Conoscere gli standard e le best practices di riferimento
- Definire un glossario per un liguaggio tecnico condiviso tra tutti i collaboratori (nessuno escluso)
- Prepare di un piano (IRP) di risposta agli incidenti con scenari operativi e gradi di responsabilità
- Analisi degli scenari ad alto rischio e frequenza (analisi log file)
- Protocollo di dialogo e interazione con i partner esterni (interoperabilità)
- Sviluppi di modelli per la messa in sicurezza dei dati sensibili per livello di rischio
- Definire un protocollo di reazione comune in funzione degli scenari sopra definiti

I 3 standard di riferimento

www.iso.org

ICS › 35 › 35.030

ISO/IEC 27035-2:2016

Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response

ICS › 35 › 35.030

ISO/IEC 27035-1:2016

Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

ICS › 35 › 35.030

ISO/IEC 27037:2012

Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

Sette suggerimenti con il lavoro ibrido

(www.cybersicuro.ch)

1) Il luogo dove depositivi i documenti è importante

Se lavori da casa, sicuramente ti hanno fornito le credenziali per collegarti alla rete aziendale attraverso una rete virtuale privata di tipo VPN (Virtual Private Network). In questo modo il trasferimento dei dati gode di un buon grado di sicurezza. Tuttavia, assicurati che i dati che salvi sul tuo apparecchio elettronico, una volta fuori dalla VPN, non vengano lasciati incustoditi in aree di lavoro non protette. Potrebbe bastare una ricerca in Google strutturata e mirata, come per esempio "*stipendi site:www.ti.ch*" per arrivare astutamente ai files dimenticati in zone non adeguatamente protette.

2) Utilizzo di memorie USB

Non collegare mai al tuo apparecchio elettronico aziendale memorie USB sconosciute trovate per casa, ricevute in regalo o prese in prestito da persone non autorizzate dall'azienda, fatta eccezione di quelle bonificate digitalmente attraverso un processo completo di formattazione avvenuto su un altro apparecchio elettronico di cui hai il controllo. Le memorie USB sono tra i maggiori vettori di contaminazione (silenziosa) dei dati, usati per introdurre maldestramente programmi malevoli. Se per necessità professionali non hai alternativa valide, assicurati prima di disporre di un antivirus valido e aggiornato allo stato dell'arte.

3) Apparecchi elettronici personali e professionali

Lavorando da casa spesso il confine che divide gli apparecchi personali da quelli ad uso professionale viene a scemare col passare del tempo. Questo a causa dalla fragile percezione che dentro casa nessuna persona indesiderata possa manipolarli fisicamente. Evita quindi di lasciare l'apparecchio elettronico professionale privo di una password di protezione. Assicurati invece che il timer di attivazione automatica della password sia impostato con un tempo relativamente breve in caso di inutilizzo dell'apparecchio elettronico.

4) Altri apparecchi elettronici casalinghi collegati

Spesso dentro casa vi sono molteplici apparecchi elettronici collegati alla rete internet casalinga, e per comodità di creano cartelle virtuali condivise in cui depositare i dati e i documenti. Per quanto comodi, ricordati di non usare mai questi spazi famigliari per depositare documenti e dati aziendali sensibili, anche solo temporaneamente. Questi sono tra i primi spazi virtuali che i programmi malevoli cercano una volta penetrati nella rete domestica.

5) Collegamenti a sistemi di cloud esterni

Utilizzare sistemi di cloud offre senza dubbio molteplici vantaggi di condivisione e accesso rapido ai dati, soprattutto a distanza, ma spesso pone di fronte a molti rischi dovuti al fatto che i sistemi di carattere gratuito dichiarano nelle condizioni d'uso di poter consultare, usare, condividere e rivendere con terze parti i dati depositati nei loro server. Questo potrebbe mettere seriamente in pericolo la reputazione del tuo datore di lavoro, oltre che la sicurezza dei dati sensibili professionali. Seppur comodi, evita in modo assoluto l'utilizzo di sistemi di cloud gratuiti o non autorizzati dall'azienda.

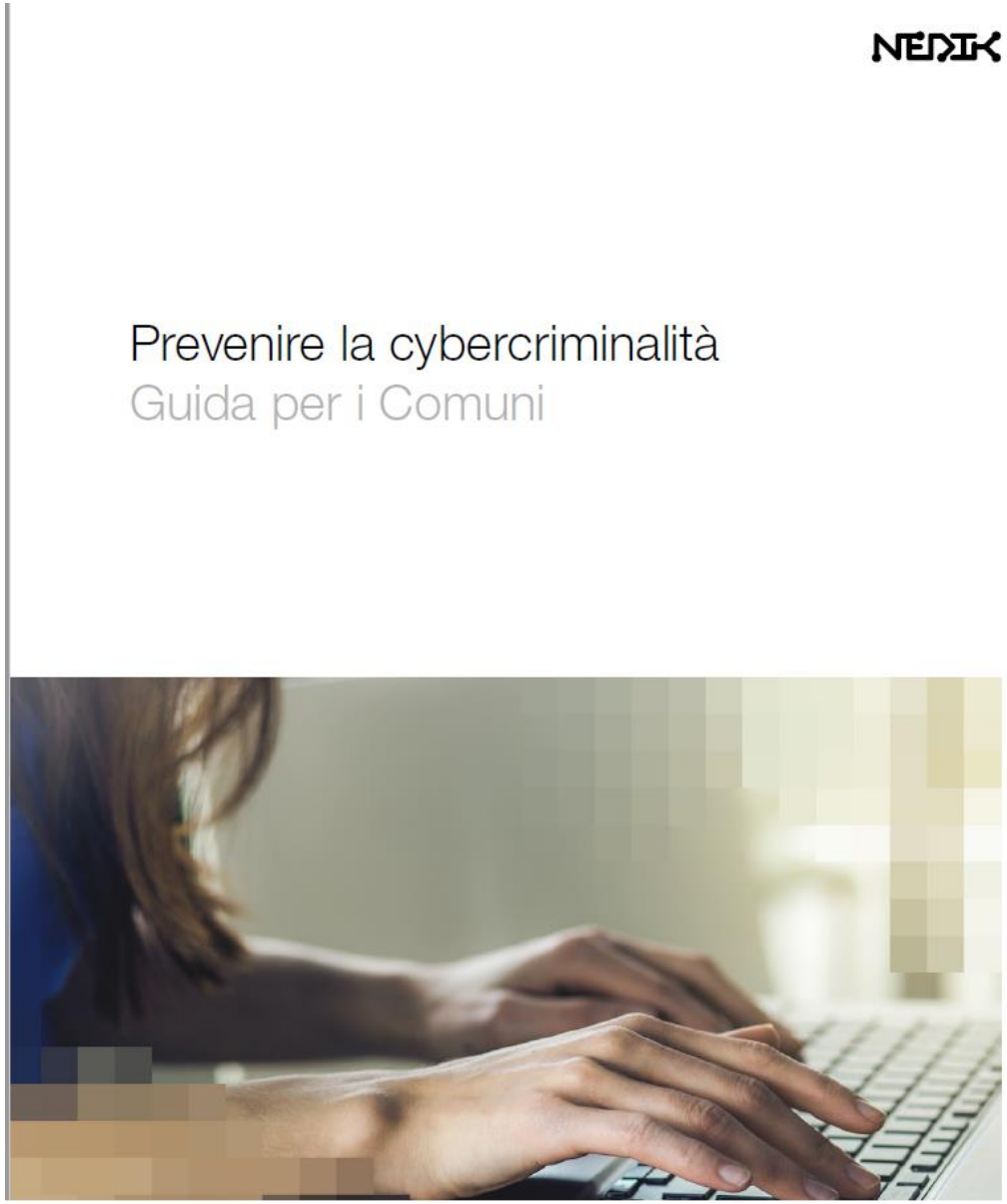
6) Aggiornamento di tutti gli apparecchi elettronici di casa

Assicurarti che tutti gli apparecchi elettronici che hai dentro casa dispongano di un antivirus adeguato e sempre aggiornato. Ne basta soltanto uno collegato alla rete domestica non adeguatamente protetto, per mettere a rischio la sicurezza di tutti gli altri apparecchi, e in particolare, per diventare un cavallo di troia per risalire e accedere a quello aziendale con i dati sensibili. Ricorda che l'arrivo del 5G potrebbe portare dentro casa oggetti ludici, come giochi per bambini, anch'essi collegati e interconnessi alla rete casalinga.

7) La sera quando termini il lavoro

La sera quando termini il lavoro assicurati che sull'apparecchio elettronico aziendale non rimangano documenti di lavoro incustoditi, per esempio sul desktop o in cartelle temporanee non adeguatamente protette. Controlla sempre di aver salvato tutti i files negli spazi virtuali appositi senza lasciare nulla in giro, anche quando la stanchezza, la fretta o la pressione potrebbero trarre in inganno.

Una guida per i Comuni



Centro nazionale per la cibersicurezza (NCSC)

Polizia cantonale di Zurigo, NEDIK

Raccomandazioni concrete per proteggersi dalla cybercriminalità

Gli attacchi informatici possono danneggiare in modo permanente la fiducia della popolazione nell'amministrazione.

https://www.svs.admin.ch

Info di contatto.

Dr.-Ing.- Alessandro Trivilini, Ph.D.

www.trivilini.info