UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Presidenza del Consiglio dei Ministri
Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

Competenze digitali per la PA

Proteggere i dati personali e la privacy

Avv. Ernesto Belisario

FormezPA

Prima di iniziare

I rischi della trasformazione digitale

La tecnologia è una cosa curiosa: ti dà grand doni in una mano e ti pugnala alle spalle con l'altra.

(Charles Percy Snow)

I rischi della trasformazione digitale

Il problema non è 'se' violeranno i nostri dati. Ma 'quando'.

(Giovanni Ziccardi)

La consapevolezza dell'importanza dei dati

L’importanza della sicurezza informatica

Le minacce alla sicurezza dei dati

Attacchi dall'esterno

- Acquisizione indebita di dati
- Sabotaggio / Spionaggio
- Corruzione dei dati

Le minacce alla sicurezza dei dati

Danni da risorse umane

- Accessi non autorizzati
- Acquisizione / Comunicazione indebita
- Perdita / Corruzione dati

Le minacce alla sicurezza dei dati

Applicazioni non affidabili

- Perdita di prestazioni
- Inibizione accesso ai dati
- Vulnerabilità sulla sicurezza / Fault operativi

La sicurezza informatica nella PA digitale

- smart working

La sicurezza informatica nella PA digitale

- servizi online

L’importanza della privacy

Con le banche dati, le reti, la tv via cavo e anche le tecnologie genetiche - che sono in gran parte raccolte di informazioni sulle persone - il diritto di privacy non è più soltanto quello di essere lasciato solo, ma anche, e soprattutto, quello di controllare il destino delle informazioni che circolano sul proprio conto.

(Stefano Rodotà)

Proteggere i dati

Le nozioni fondamentali

Saper distinguere tra

- integrità
- non ripudio
- riservatezza

La normativa di riferimento

Gazzetta ufficiale L 119

dell'Unione europea

Edizione in lingua italiana

Legislazione

59° anno

4 maggio 2016

Sommario

I *Atti legislativi*

REGOLAMENTI

★ **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)** (1) 1

Reg. UE 2016/679 (GDPR)

La finalità del GDPR

Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

Art. 1, par. 1, GDPR

Ambito di applicazione del GDPR

Il GDPR si applica

- ☑ *alle persone fisiche e al trattamento interamente o parzialmente automatizzato dei dati personali e al trattamento non automatizzato di dati contenuti in archivio o destinati a figurarvi.*

Non si applica, invece:

- ☐ *ai trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;*
- ☐ *ai dati anonimi.*

Conoscere le norme e i principi da seguire

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, par. 1, GDPR

Dato sensibile

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 a 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, GDPR

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.

Art. 4, par. 1, GDPR

I principi da seguire

Il titolare del trattamento è competente per il rispetto dei principi previsti dal GDPR e in grado di comprovarlo (c.d principio di «responsabilizzazione»).

Art. 5, par. 2, GDPR

I principi da seguire

I dati personali sono

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (liceità, correttezza e trasparenza);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali (limitazione della finalità);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);

I principi da seguire

I dati personali sono

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (minimizzazione dei dati);
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (esattezza);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

I principi da seguire

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Art. 25, par. 1 GDPR

I principi da seguire

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Art. 25, par. 2 GDPR

INTERMEDIATE LEVEL

ADVANCED LEVEL

Proteggere i dati nella PA digitale

Gli adempimenti

1. Mappatura delle attività di trattamento e tenuta del registro
2. Conduzione dell'analisi del rischi in relazione al trattamento
3. Conduzione di valutazione d'impatto (DPIA) per i trattamenti più rischiosi
4. Scelta dei fornitori che forniscano garanzie in tema di sicurezza (e loro nomina quali responsabili del trattamento)
5. Adozione di misure di sicurezza tecniche organizzative
6. Adozione procedure per incidenti informatici e data breach
7. Pubblicazione delle informative per gli utenti

Le misure di sicurezza

Misure Tecniche

La misura tecnica è affidata ad uno strumento, ad una macchina o ad un elaboratore. La conformità in questo caso, dipende dalla correttezza della programmazione della macchina e della sua funzionalità.

Esempi di misure tecniche:

Pseudonimizzazione (Encryption; Masking; Tokenizzazione)

Misure Organizzative

La misura organizzativa è affidata ai comportamenti delle persone, conformi ad uno standard operativo codificato in regole aziendali/protocolli operativi.

Esempi di misure organizzative:

- Controlli degli accessi
- Controlli dei supporti cartacei
- Protezione ambienti e risorse di rete
- Gestione della password

Il CAD e i provvedimenti attuativi

Con le Linee guida sono individuate le soluzioni tecniche idonee a garantire la protezione, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati e la continuità operativa dei sistemi e delle infrastrutture. 1-bis. AgID attua, per quanto di competenza e in raccordo con le altre autorità competenti in materia, il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la sicurezza cibernetica e la sicurezza informatica. AgID, in tale ambito:
a) coordina, tramite il Computer Emergency Response Team Pubblica Amministrazione (CERT-PA) istituito nel suo ambito, le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la semplificazione e la pubblica amministrazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.

Art. 51, comma 1, CAD

Il CAD e i provvedimenti attuativi

- *Circolare Agid n. 2/2017 sulle misure minime di sicurezza ICT*
- *Linee Guida Agid sui profili di sicurezza negli acquisti ICT*

Lavorare in sicurezza

Per approfondire

Protezione dei dati personali

- Reg. UE 2016/679 (GDPR)
  eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A32016R0679

- Autorità Garante per la protezione dei dati personali
  www.garanteprivacy.it

- Comitato europeo per la protezione dei dati
  edpb.europa.eu/edpb_it

Sicurezza nella PA digitale

- Cert-Agid
  www.agid.gov.it/it/sicurezza/cert-agid

- Circolare Agid n. 2/2017
  www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

- Linee guida Agid sulla sicurezza degli acquisti ICT
  www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2020/05/20/sicurezza-procurement-ict-online-linee-guida

Sicurezza nello smart working

- Vademecum Agid per smart working in sicurezza
  www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2020/03/17/smart-working-vademecum-lavorare-online-sicurezza

- Il decalogo dello smart worker (laPAdigitale)
  www.lapadigitale.it/wp-content/uploads/decalogo_smart_worker.jpg

- Guida pratica al lavoro agile nella PA
  www.funzionepubblica.gov.it/articolo/dipartimento/12-03-2020/guida-pratica-al-lavoro-agile-nella-pa

Competenze digitali per la PA

GRAZIE PER L'ATTENZIONE

ebelisario@e-lex.it

FormezPA