Il Piano di Sicurezza & Privacy di un'Autorità Indipendente

20 Maggio 2019

Dott. Giovanni OLIVE (PMP, CISA)
Autorità Nazionale Anticorruzione
Ufficio Programmazione e Sviluppo delle Banche Dati,
Piattaforma Digitale e Servizi IT

Abstract

Dal 2016, la Pubblica Amministrazione italiana ha cominciato ad interrogarsi su come poter adempiere alle misure dettate dalla normativa europea UE 679/2016 (GDPR), dovendo considerare una serie di difficoltà quali, ad esempio, i tanti vincoli di bilancio dettati dalla perdurante crisi economica e dalla sempre crescente necessità di tagliare i costi di gestione e di investimento. Alle difficoltà economiche si devono sicuramente aggiungere le normative con impatto tecnico-organizzativo intervenute negli ultimi anni e che hanno inflazionato gli interventi a carico delle stesse. Queste problematiche hanno costretto molte PP.AA. a lavorare sugli adempimenti del GDPR in maniera graduale ed assegnando delle priorità agli interventi. Il seminario descrive le varie fasi del piano biennale di adeguamento al GDPR di un'Autorità Indipendente.

Il percorso descrittivo inizia presentando l'Autorità le proprie peculiarità istituzionali dell'Autorità, proseguendo con l'analisi e le riflessioni sulle esperienze maturate nel campo della Cybersecurity e della normativa Privacy fino ad arrivare a proporre una riflessione tecnica ed organizzativa di automazione degli adempimenti richiesti dalla GDPR. Nella prima parte si affronteranno i temi riguardanti il contesto normativo, l'organizzazione e gli attori coinvolti, proseguendo con la descrizione dell'approccio e delle soluzioni adottate. In conclusione si condivideranno le criticità affrontate e le sfide future.

Mission

può essere individuata nella prevenzione della corruzione nell'ambito delle amministrazioni pubbliche, nelle società partecipate e controllate anche mediante l'attuazione della trasparenza in tutti gli aspetti gestionali, nonché mediante l'attività di vigilanza nell'ambito dei contratti pubblici, degli incarichi e comunque in ogni settore della pubblica amministrazione che potenzialmente possa sviluppare fenomeni corruttivi, evitando nel contempo di aggravare i procedimenti con ricadute negative sui cittadini e sulle imprese, orientando i comportamenti e le attività degli impiegati pubblici, con interventi in sede consultiva e di regolazione, non chè mediante attività conoscitiva.

La base giuridica

La Legge 6 novembre 2012, n. 190 (Legge Severino) "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"

Il decreto legge 24 giugno 2014 n. 90, convertito in legge n. 114/2014.

Principali compiti

Contratti pubblici

Prevenzione della corruzione

Trasparenza

Regolazione e vigilanza

Ruolo

Decreto Legislativo 50/2016 , Codice dei Contratti Pubblici art. 213

…garantisce la promozione dell'efficienza, della qualità dell'attività delle stazioni appaltanti, *cui fornisce supporto anche:*

- ***facilitando lo scambio di informazioni***
- ***omogeneità dei procedimenti amministrativi***
- ***favorendo lo sviluppo delle migliori pratiche*.**

Per queste finalità, *l'Autorità gestisce la Banca Dati Nazionale dei Contratti Pubblici, nella quale confluiscono, oltre alle informazioni acquisite per competenza tramite i propri sistemi informatizzati, tutte le informazioni contenute nelle banche dati esistenti, per garantire: accessibilità unificata, trasparenza, pubblicità e tracciabilità delle procedure di gara*

Settori ed ambiti Interesse

eProcurement

- Sistema Informativo Monitoraggio Gare (SIMOG)
- Portale dei bandi e dei contratti pubblici
- AVCpass
- Anagrafe Unica delle Stazioni Appaltanti (AUSA)
- Annotazioni riservate
- Casellario delle imprese
- Certificati Esecuzione Lavori
- Adempimenti Legge 190/2012 art. 1, comma 32
- Elenco società in house
- Servizio Riscossione Contributi
- Società di ingegneria e professionali
- Società Organismo di Attestazione (SOA)

Anticorruzione

- Servizi Anticorruzione e Trasparenza
- Segnalazione di condotte illecite – Whistleblowing
- Responsabili della Prevenzione della Corruzione e della Trasparenza
- Campagna trasparenza –
- Quesiti, Segnalazioni e Proposte in materia di Trasparenza (d.lgs. n. 33/2013)
- Portale della performance

Base Dati Nazionale Contratti Pubblici

BDNCP – Banca Dati Nazionale dei Contratti Pubblici

decreto legislativo 7 marzo 2005, n. 82 Codice dell'Amministrazione Digitale

Art. 62-bis. Banca dati nazionale dei contratti pubblici.

1. Per favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi ed assicurare l'efficacia, la trasparenza e il controllo in tempo reale dell'azione amministrativa per l'allocazione della spesa pubblica in lavori, servizi e forniture, anche al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e prevenire fenomeni di corruzione, si utilizza la «Banca dati nazionale dei contratti pubblici» (BDNCP) gestita dall'Autorità Nazionale Anticorruzione ai sensi dell'articolo 213 del decreto legislativo 18 aprile 2016, n. 50.

BDNCP

BDNCP raccoglie ed integra i dati trasmessi dalle stazioni appaltanti riguardanti il ciclo di vita dei contratti pubblici da queste gestiti, dalla pubblicazione della gara al suo affidamento, alla sottoscrizione del o dei contratti ed alla loro esecuzione.

In cifre:

- Circa 1.000.000 di CIG rilasciati ogni anno per gare sopra i 40.000 euro
- 285.000 utenti attivi
- 40000 stazioni appaltanti organizzate in 200.000 centri di costo
- BDNCP fornisce i dati ad AVCpass fino all'entrata in funzione della BDOE
- 200.000 Operatori Economici
- 40.000.000 Contratti registrati in BDNCP, alimentata da SiMOG
- 6.000.000 di gare sopra i 40.000 € registrate attraverso Simog
- 34.000.000 di contratti sotto i 40.000 €

Sorgenti di dati

Operatori Economici

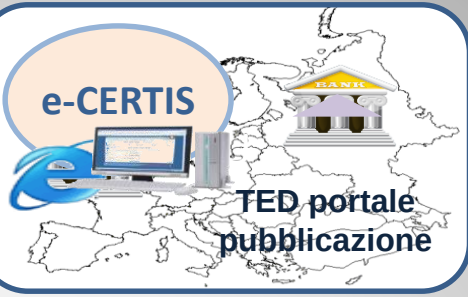
Stazioni Appaltanti

Pubbliche Amministrazioni

Servizi per la raccolta dati

PIATTAFORME E-procuremnt

e-CERTIS



TED portale pubblicazione

Servizi di interoperabilità

BDNCP

Servizi per l'accesso libero ai dati

Servizi per l'accesso ai dati

Fruitori dei dati

CdC DIA etc

BDAP

MEF

DAF

BDOE

Soggetti Aggregatori

Nodo Scambio Ordini RGS

Imprese

Pubbliche Amministrazioni

Cittadini

LE ESIGENZE ALLA BASE DELLA RIFORMA

Obiettivo: Consentire ai cittadini europei di riprendere il controllo dei propri dati personali.

- **Due terzi degli europei (67%), secondo un sondaggio di Eurobarometer, hanno dichiarato di essere preoccupati di non avere il controllo completo sulle informazioni fornite online.**

- **Sette europei su dieci si preoccupano del potenziale uso che le società potrebbero fare delle informazioni divulgate**

- **La riforma della protezione dei dati consente di rafforzare il diritto alla protezione dei dati, che è un diritto fondamentale nell'UE, e consente ai cittadini di avere fiducia quando conferiscono i loro dati personali.**

Diritti rafforzati per i cittadini

LE NUOVE REGOLE RAFFORZANO I DIRITTI ESISTENTI E RESPONSABILIZZANO GLI INDIVIDUI AD UN MAGGIORE CONTROLLO SUI LORO DATI PERSONALI. IN PARTICOLARE:

- **più facile accesso ai propri dati: le persone avranno maggiori informazioni su come vengono elaborati i loro dati e queste informazioni dovranno essere disponibili in modo chiaro e comprensibile;**
- **il diritto alla portabilità dei dati: sarà più facile trasferire i dati personali tra i fornitori di servizi;**
- **Il "diritto all'oblio": quando non si desidera più che i propri dati vengano elaborati. A condizione che non vi siano motivi legittimi per mantenerli, i dati dovranno essere cancellati;**
- **il diritto di sapere se i propri dati sono stati violati: le aziende e le pubbliche amministrazioni devono notificare quanto prima all'autorità di vigilanza nazionale gravi violazioni dei dati, in modo che gli utenti possano prendere le misure appropriate.**

Nuove regole

Nell'odierna economia digitale, i dati personali hanno acquisito un enorme significato economico, in particolare nel settore dei big data.

Unificando le regole europee sulla protezione dei dati, il legislatore europeo ha inteso favorire le opportunità di business e incoraggiare l'innovazione.

- **"One continent - one law": il regolamento stabilirà un'unica serie di norme che renderà più semplice e meno costoso per le imprese fare affari nell'UE.**
- **"One-stop-shop": le aziende dovranno trattare con un'unica autorità di vigilanza. Si stima che ciò consentirà di risparmiare 2,3 miliardi di euro all'anno.**
- **Norme europee sul suolo europeo. Le società con sede al di fuori dell'Europa, dovranno applicare le stesse regole quando offrono servizi nell'UE.**
- **Approccio basato sul rischio: le regole dovranno essere calibrate sui rispettivi rischi.**
- **Regole adatte all'innovazione: il regolamento garantirà che le misure per la protezione dei dati siano incorporate nei prodotti e nei servizi fin dalle prime fasi di sviluppo (privacy by design).**

APPROCCIO BASATO SUL RISCHIO
MISURA DI ACCOUNTABILITY PER TITOLARI E RESPONSABILI

- **Adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (Cfr.: Capo IV - Titolare del trattamento e responsabile del trattamento)**

- **Ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali (nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento)**

  - **Data protection by default and by design**
  - **Analisi del rischio del trattamento**
  - **Misure di sicurezza idonee**
  - **Gestione dei data Breaches**
  - **Approccio "proattivo" alla protezione dei dati personali**

GDPR Novità e principali adempimenti

NOVITA' GDPR

Data Breach

- **Notifica al Garante Privacy entro 72 ore.**

Certificazioni Privacy

- **Il GDPR promuove la definizione ed utilizzo di Certificazioni Privacy (misure di sicurezza da pare di Titolari e Responsabili, Trasferimento dati extra UE,…).**
- **La certificazione non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti.**

Responsabile della protezione dei dati/Data Protection Officer

- **Nuova figura obbligatoria per le pubbliche amministrazioni. Ruolo caratterizzato da indipendenza e autonomia decisionale**

ART. 5 PRINCIPI

Paragrafo 1)

- **liceità, correttezza e trasparenza**
- **limitazione della finalità**
- **minimizzazione dei dati**
- **esattezza**
- **limitazione della conservazione**
- **integrità e riservatezza**

Paragrafo 2)

«Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo»

Art. 6 LICEITA'

Il GDPR conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica

I fondamenti di liceità del trattamento sono indicati all'art. 6 del GDPR:

- **consenso,**
- **adempimento obblighi contrattuali,**
- **interessi vitali della persona interessata o di terzi,**
- **obblighi di legge cui è soggetto il titolare,**
- **interesse pubblico o esercizio di pubblici poteri,**
- **interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati**

l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle pubbliche amministrazioni in esecuzione dei rispettivi compiti.

LICEITA'

INTERESSE PUBBLICO O ESERCIZIO DI PUBBLICI POTERI

DISPOSIZIONI

La finalità del trattamento …..per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

La base giuridica stabilita da norma di legge o regolamento (diritto UE o Italiano) potrebbe contenere:

- le **condizioni generali** relative alla liceità del trattamento da parte del titolare del trattamento;
- le **tipologie di dati** oggetto del trattamento; gli interessati;
- i **soggetti cui possono essere comunicati** i dati personali e le finalità per cui sono comunicati;
- le **limitazioni** della finalità,
- i **periodi di conservazione** e le operazioni e procedure di trattamento, comprese **le misure attea garantire un trattamento lecito e corretto**, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX.

IMPATTI

Ai fini del rispetto del principio di Liceità dei trattamenti è opportuno **verificare la base giuridica** stabilita dal diritto dell'Unione o dal diritto dello Stato italiano secondo la quale si effettuano i trattamenti rilevando le relative specifiche. Per tutti i nuovi trattamenti dovranno essere verificate le relative basi giuridiche.

Responsabilità

Ogni ufficio per i trattamenti di dati personali di competenza

RPD e Gruppo GSP

Supportano gli uffici nell'applicazione del Regolamento

INFORMATIVA
Art. 13 e 14

DISPOSIZIONI

I contenuti dell'informativa sono elencati in modo e in parte sono più ampi rispetto al Codice. Si deve sempre specificare:

- i dati di contatto del **RPD**
- **la base giuridica** del trattamento,
- qual è il suo interesse legittimo (se quest'ultimo costituisce la base giuridica del trattamento)
- **se trasferisce i dati personali in Paesi terzi** e con quali strumenti (es: clausole contrattuali modello).
- **il periodo di conservazione dei dati** (o i criteri seguiti per stabilire tale periodo di conservazione)
- **il diritto di presentare un reclamo all'autorità di controllo**.
- **Se il trattamento comporta processi decisionali automatizzati** (ad es: profilazione) deve indicare la logica di tali processi decisionali e le conseguenze previste per l'interessato.

IMPATTI

È necessario **verificare la rispondenza delle informative** attualmente utilizzate alle nuove disposizioni con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche o le integrazioni eventualmente necessarie prima del 25 maggio 2018.

DIRITTO ALLA CANCELLAZIONE (OBLIO) (ART. 17)

DISPOSIZIONI

- Il diritto cosiddetto “all’oblio” si **configura come un diritto alla cancellazione** dei propri dati personali in forma rafforzata.
- Si prevede, l’obbligo per i titolari (se hanno “reso pubblici” i dati personali dell’interessato ad esempio, pubblicandoli su un sito web) di **informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati**, compresi **“qualsiasi link, copia o riproduzione”**
- I titolare adotta le **misure ragionevoli**, anche tecniche, tenendo conto della tecnologia disponibile e dei costi di attuazione

IMPATTI

E’ necessario **avere pronto un processo specifico** per poter dare riscontro alle richieste di cancellazione.

RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO (Art. 24)

DISPOSIZIONI

Responsabilità del titolare del trattamento

*1. Tenuto conto della **natura**, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei **rischi aventi probabilità e gravità diverse** per i **diritti e le libertà delle persone fisiche**, il titolare del trattamento **mette in atto misure tecniche e organizzative** adeguate **per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento**.*

Dette misure sono riesaminate e aggiornate qualora necessario.

Principali Adempimenti

- Registro delle attività di trattamento (art. 30);
- Valutazione di impatto e consultazione preventiva (artt. 35 -36);
- Responsabile della protezione dei dati (artt. 37-39);
- Sicurezza dei dati personali (artt. 32-34).

IMPATTI

Tutti gli Uffici, i Responsabili del trattamento e la struttura organizzativa di coordinamento ed impulso delle attività (Gruppo GSP, Responsabile della protezione dei dati) debbono **supportare secondo competenza l'applicazione del Regolamento**

RESPONSABILE DEL TRATTAMENTO
Articolo 28

DISPOSIZIONI

- I Responsabili debbono **presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** affinché il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.
- Il responsabile del trattamento **può ricorrere a un altro responsabile previa autorizzazione scritta, specifica o generale, del titolare del trattamento**.
- I trattamenti da parte di un responsabile del trattamento **sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri,** che vincoli il responsabile del trattamento al titolare del trattamento
- Il contratto **stipula la materia disciplinata** e **la durata del trattamento**, la **natura e la finalità del trattamento**, il **tipo di dati** personali e **le categorie di interessati,** gli **obblighi e i diritti del titolare del trattamento.**

IMPATTI

adeguare le nomine dei responsabili esterni alle nuove disposizioni regolamentari con particolare riferimento all'art. 28, paragrafo 3, del regolamento

Principali Adempimenti

- Registro delle attività di trattamento (art. 30);
- Valutazione di impatto e consultazione preventiva (artt. 35 -36);
- Responsabile della protezione dei dati (artt. 37-39);
- Sicurezza dei dati personali (artt. 32-34).

RESPONSABILE DELLA PROTEZIONE DEI DATI (Art, 37, 38, 39)

DISPOSIZIONI

- **Il responsabile della protezione dei dati** è incaricato almeno dei seguenti compiti:

  a) informare e **fornire consulenza** al titolare o al responsabile del trattamento

  b) **sorvegliare l'osservanza del presente regolamento**,

  c) fornire, se richiesto, un **parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento

  d) **cooperare con l'autorità di controllo**;

  e) fungere da **punto di contatto per l'autorità di controllo**

  Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

  Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati **sia tempestivamente e adeguatamente coinvolto in tutte le questioni** riguardanti la protezione dei dati personali e **che non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti**. Il responsabile della protezione dei dati **non è rimosso o penalizzato per l'adempimento de propri compiti.**

IMPATTI

Procedere con la nomina ed inserire tale nuova figura nel Sistema di gestione di sicurezza e privacy

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

Articolo 35

DISPOSIZIONI

Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, **può presentare un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

IMPATTI

L'ammnistrazione deve sviluppare un processo di valutazione di impatto sulla protezione dei dati prima di iniziare nuovi trattamenti di dati che possano comportare un elevato rischio per l'interessato.

NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL' AUTORITÀ DI CONTROLLO (Art. 33)

DISPOSIZIONI

il titolare del trattamento nel caso di violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, è tenuto a notificare la violazione all'autorità di controllo competente **entro 72 ore**.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica di cui al paragrafo deve almeno:

a) descrivere la **natura della violazione** ove possibile le categorie e il **numero approssimativo di interessati**, le **categorie** e il **numero** approssimativo di **registrazioni dei dati** personali in questione;

b) comunicare il nome e i dati di **contatto del RPD** o di altro punto di contatto presso cui ottenere più informazioni;

c) descrivere le probabili **conseguenze della violazione dei dati** personali;

d) descrivere le **misure adottate/proposte per porre rimedio** alla violazione per attenuarne i possibili effetti negativi.

Il titolare è tenuto a **documentare qualsiasi violazione dei dati** personali. La documentazione consente all'autorità di controllo di verificare il rispetto di tale disposizione

IMPATTI

Definire il processo e la procedura operativa che dettaglia ruoli e meccanismi decisionali nel caso si verifichino violazioni di dati personali che richiedano la comunicazione al Garante Privacy.

Deve essere messa in campo anche una procedura di documentazione di tutte le violazioni di dati personali eventualmente occorse.

COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO (Art. 34)

DISPOSIZIONI

Se la violazione suscettibile di **presentare un rischio elevato per i diritti e le libertà delle persone fisiche**,

La comunicazione all'interessato **descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali** e contiene almeno le seguenti informazioni

- il nome e i dati di contatto del RPD o di altro punto di contatto presso cui ottenere più informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate/proposte per porre rimedio alla violazione per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) Presenza le **misure** tecniche e organizzative adeguate

b) Adottate misure atte a scongiurare il **sopraggiungere di un rischio elevato** per i diritti e le libertà degli interessati

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

IMPATTI

Definire il processo e la procedura operativa che dettaglia ruoli e meccanismi decisionali nel caso si verifichino violazioni di dati personali che richiedano la comunicazione anche all'interessato

MISURE DI SICUREZZA
(Art. 32)

DISPOSIZIONI

a) la **pseudonimizzazione** e la **cifratura**

b) assicurare su **base permanente la riservatezza, l'integrità, la disponibilità e la resilienza** dei sistemi e dei servizi di trattamento;

c) la **capacità di ripristinare tempestivamente la disponibilità e l'accesso** dei dati personali in caso di incidente fisico o tecnico;

d) una **procedura per testare**, verificare e valutare regolarmente **l'efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

2. Nel **valutare l'adeguato livello di sicurezza**, si tiene conto in special modo dei **rischi** presentati dal trattamento che derivano in particolare dalla **distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.**

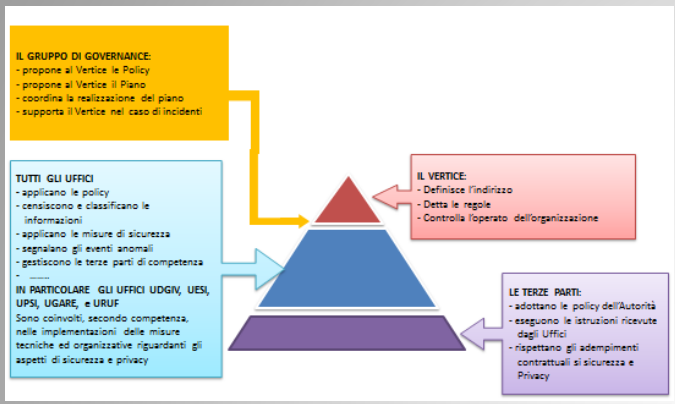
3. **Codice di condotta o meccanismi di certificazione** (art.42) possono essere utilizzati come elemento **per dimostrare la conformità** ai requisiti di cui al paragrafo 1 dell'articolo 32

4. **Il titolare del trattamento e il responsabile del trattamento** fanno sì che **chiunque agisca sotto la loro autorità** e abbia accesso a dati personali **non tratti tali dati se non è istruito in tal senso dal titolare** del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri

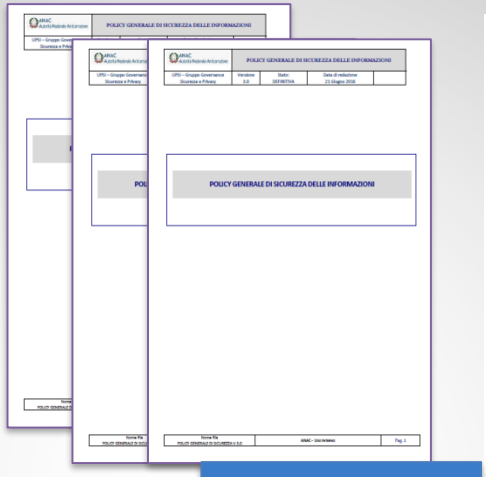
IMPATTI

Messa in campo del modello gestionale al fine di perseguire gli obiettivi di protezione dell'Art. 32

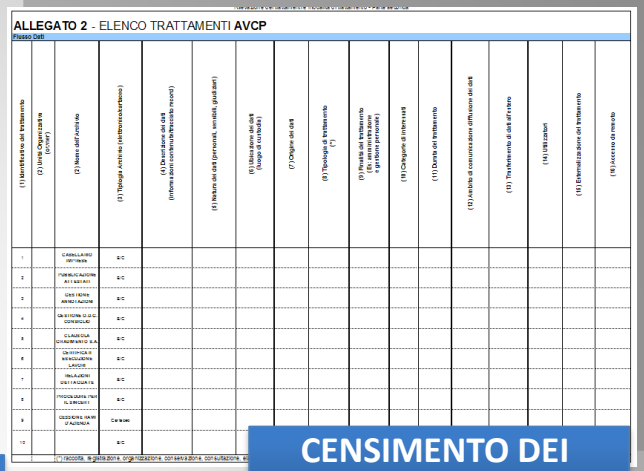
COMPONENTI DEL SISTEMA DI GESTIONE



ORGANIZZAZIONE GESTIONE PRIVACY



POLICY



CENSIMENTO DEI DATI PERSONALI

Minacce	Probabilità	Gravità	Rischio
Disastri naturali (terremoti, uragani, inondazioni, caduta di fulmini)	B	A	MEDIO
Incendio	B	B	BASSO
Danneggiamento intenzionale	B	M	BASSO
Azione di spionaggio industriale	B	M	BASSO
Attacco terroristico	B	B	BASSO
Guasto infrastrutture (energia elettrica, condizionamento)	B	B	BASSO
Guasto Hardware	B	A	MEDIO
Guasto Software	B	A	MEDIO
Guasto di componenti di rete	B	M	BASSO
Utilizzo di software da parte di soggetti non autorizzati	B	A	BASSO
Furto	A	A	ALTO
Sottrazione di credenziali di autenticazione	B	M	BASSO
Intercettazione di traffico	B	A	MEDIO
Intrusione in rete	B	A	MEDIO
Accesso logico non autorizzato	M	A	MEDIO
Uso non autorizzato di supporti di memorizzazione	M	A	ALTO
Utilizzo illegale di software	B	B	BASSO
Virus, Software 'malicious'	A	B	MEDIO
Import/export illegale di software	B	B	BASSO
Mascheramento di identità dell'utente			
Accesso alla rete da parte di utenti non autorizzati			
Utilizzo non autorizzato di apparati di rete			
Errore operatore			
Errore utente			

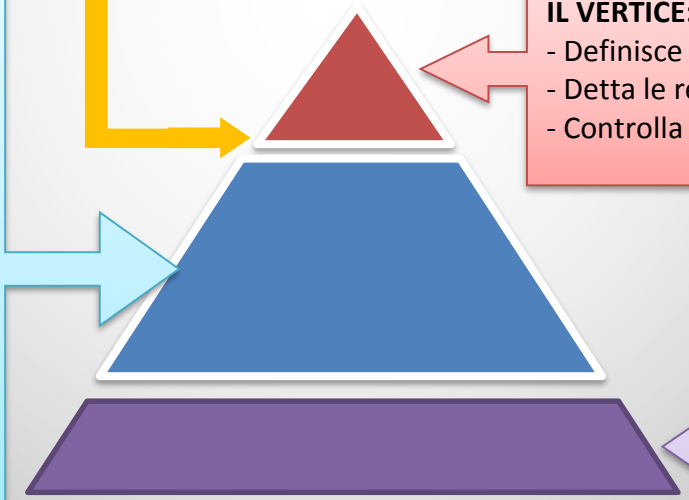
ANALISI E GESTIONE DEI RISCHI

PIANO DELLE MISURE

ORGANIZZAZIONE PER LA GESTIONE DELLE TEMATICHE DI SICUREZZA DELLE INFORMAZIONI E TUTELA DEI DATI PERSONALI

IL GRUPPO DI GOVERNANCE:
- propone al Vertice le Policy
- propone al Vertice il Piano
- coordina la realizzazione del piano
- supporta il Vertice nel caso di incidenti

IL VERTICE:
- Definisce l'indirizzo
- Detta le regole
- Controlla l'operato dell'organizzazione



TUTTI GLI UFFICI
- applicano le policy
- censiscono e classificano le informazioni
- applicano le misure di sicurezza
- segnalano gli eventi anomali
- gestiscono le terze parti di competenza
- ……..

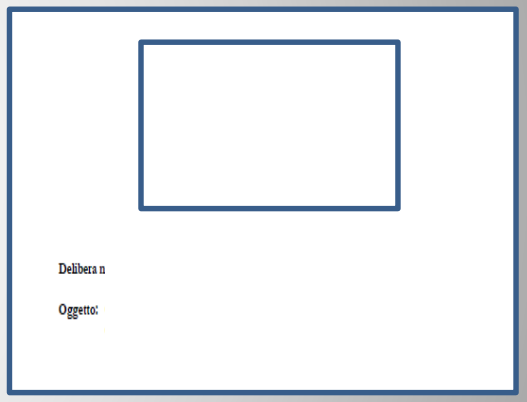
LE TERZE PARTI:
- adottano le policy dell'Autorità
- eseguono le istruzioni ricevute dagli Uffici
- rispettano gli adempimenti contrattuali si sicurezza e Privacy

ATTUAZIONE – Responsabilità, Risorse e Percorso

L' "ACCOUNTABILITY" DELL'ORGANIZZAZIONE

	TUTTI GLI UFFICI CHE EFFETTUANO TRATTAMENTI DI DATI PERSONALI	GSP UFFICI "TECNICI" (UESI, UPSIT, UGARE, URU)	GSP	RPD	RESPONSABILI DEL TRATTAMENTO (TERZE PARTI)	TITOLARE
	COMPETENZA SUI TRATTAMENTI	SUPPORTO TECNICO	GOVERNANCE	ADVISORY VERSO IL TITOLARE	INIZIATIVA SU IMPEGNO CONTRATTATUALE	INDIRIZZO E CONTROLLO
RISK MANAGMENT	♦	♦	♦	♦	♦	♦
DATA PROTECTION BY DESIGN E BY DEFAULT	♦	♦	♦	♦	♦	♦
PRIVACY IMPACT ASSESSMENT	♦	♦	♦	♦	♦	♦
DATA BREACHES	♦	♦	♦	♦	♦	♦
MISURE DI SICUREZZA E ALTRI ADEMPIMENTI	♦	♦	♦	♦	♦	♦

IL NUOVO APPROCCIO NECESSARIO PER LA CONFORMITÀ AL REGOLAMENTO . UN ESEMPIO

ESIGENZA	NUOVO APPROCCIO	ATTIVITA CONFORME
Es: Regolare attraverso una Delibera l'accesso ad una specifica tipologia di dati personali	• **Principi Privacy** • **PbD** • **Misure di sicurezza** • **……**	 Delibera n Oggetto:

RISORSE E PERCORSO

- Risorse:
  - Personale
  - Formazione
  - Mezzi tecnici
- Percorso (traguardo 25 Maggio 2018)
  - Coinvolgimento di tutti gli Uffici nel percorso di adeguamento
  - Nomina del RPD
  - Nuovo ruolo del GSP
  - Attuazione del Piano Sicurezza e Privacy (2017 e 2018)

Il Piano di Sicurezza & Privacy

Presentata un'analisi di natura tecnico-organizzativa dell'Autorità:

- organizzazione degli uffici e delle rispettive attività,
- tipologia dei dati utilizzati e loro valore ai fini del perseguimento delle attività istituzionali,
- servizi e strumenti tecnologici
- analisi dei rischi che incombono sui dati finalizzata ad identificare le misure di sicurezza e di tutela dei dati personali al fine di ridurre il rischio di violazioni di sicurezza delle informazioni e dell'ottemperanza alle vigenti disposizioni in materia di sicurezza informatica e di trattamento dei dati personali.

Le misure sono articolate in un piano d'azione che identifica le misure da applicare, i responsabili dell'attuazione ed i relativi tempi di attuazione

Il Piano di Sicurezza & Privacy

Sezione I

Adempimenti generali (informativa e consenso al trattamento) e Misure minime di sicurezza di cui all'allegato B del Codice Privacy. L'applicazione di tali misure tutela l'Autorità da sanzioni anche di natura penale previste in caso di non ottemperanza alla vigente normativa Privacy.

Sono identificate ***34 misure*** **di sicurezza** per le quali è stato necessario verificare la completa attuazione e, per quelle già attuate, prevederne il monitoraggio continuo.

Il Piano di Sicurezza & Privacy

Sezione II

Misure idonee di sicurezza, ai sensi dell'art. 31 "obblighi di sicurezza" del Codice Privacy. Per tali obblighi sono stati presi a riferimento gli obiettivi di controllo dello standard ISO 27001, in quanto migliori pratiche riconosciute a livello internazionale per garantire la sicurezza delle informazioni, al fine di ridurre i rischi di sanzioni e delle responsabilità conseguenti alla mancata attuazione di tali misure di sicurezza. Sono identificate le principali misure di controllo da attuare al fine di costituire il necessario sistema di protezione dei dati e delle informazioni trattate dall'Autorità.

Il Piano di Sicurezza & Privacy

Sezione III

Misure sicurezza da attuare ai sensi della circolare 17 marzo 2017, n. 1/2017 dell'Agenzia per l'Italia Digitale (AGID) recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni". Tale circolare prevede l'attuazione, come livello minimo obbligatorio, di ***45 misure di sicurezza*** ICT per tutte le pubbliche amministrazioni. La loro attuazione dev'essere completata entro il 31.12.2017. Alcune di tali misure possono essere ricondotte parzialmente a quelle previste nella sezione I e II del piano

Il Piano di Sicurezza & Privacy

Sezione IV

Adempimenti al Regolamento UE 2016/679. In questa sezione sono stati identificate ***32 principali "misure"*** Privacy nella direzione di una maggiore Accountability dell'organizzazione prevista dal Regolamento e riferibili a tre gruppi di misure:

- "liceità e correttezza del trattamento"
- "adeguate garanzie di sicurezza"
- "obblighi di compliance".

Metodologia di rilevazione dei Trattamenti

Partendo dai processi amministrativi dell'Autorità, sono state, in successione, individuate e classificate, le strutture dati di interesse ai fini della privacy.

Per ogni una di esse sono state rilevate le modalità e le tecnologie adottate ai fini del loro trattamento.

Viene quindi presentata una valutazione dei rischi di distruzione e perdita dei dati (anche accidentale), di accessi non autorizzati, di trattamenti non consentiti o non conformi rispetto alle finalità della raccolta, che gravano sul patrimonio informativo da tutelare.

Metodologia di rilevazione dei Trattamenti

- soggetti che utilizzano o trattano i dati a diverso titolo, quali gli incaricati o soggetti terzi anche esterni all'Azienda;
- ambito di comunicazione dei dati;
- responsabilità interne o esterne preposte al trattamento;
- modalità di trattamento elettronico e/o cartaceo;
- aree di localizzazione delle basi dati, locali in cui avvengono i trattamenti e meccanismi di sicurezza implementati.

Valutazione dei Rischi

L'analisi dei rischi a cui è esposto il patrimonio informativo dell'Autorità è stata condotta avvalendosi di:

- evidenze emerse da interviste con il personale utente
- dagli addetti alla gestione dei sistemi e delle reti
- dalla relativa documentazione disponibile;

"best practice" metodologiche basate su standard internazionali.

Livello di Maturità

- Valutazione sulla base dello standard ISO/IEC 21827 (General Requirements for Certification in Systems Security Engineering and the Systems Security Engineering- Capability Maturity Model) legata alle modalità con cui il macro processo di gestione della sicurezza delle informazioni viene messo in campo relativamente al dominio di indagine focalizzato. La scala va da un minimo di 0 (gestione assente) ad un massimo di 5 (gestione ottimale con processi di miglioramento continuo in atto).

PRISMA@PA

PRIvacy Services MAnagement-Public Administration

SCENARIO

AMBITO DI RIFERIMENTO
La Pubblica Amministrazione

Il BIG BANG
Il regolamento generale per la protezione dei dati personali

Obiettivo: compliance
La PA "stretta" fra GDPR, Agenda Digitale e tagli di spesa

+ **REALTÀ OPERATIVA** e **IDEA PROGETTUALE**
+ Accountability *vs* Misure Minime
+ Dal Censimento dei Trattamenti (in Excel) al Sistema di gestione

LA PROPOSTA

PRISMA @PA

PRISMA@PA *VS* ACCOUNTABILITY

ACCOUNTABILITY

E' difficile coglierne il senso nella pratica, date le molte declinazioni del termine. Di certo è riduttivo interpretarlo come "responsabilità".

L'ACCOUNTABILITY NELL'ECONOMIA DELLE P.A.

"rendere conto" delle scelte operate nell'utilizzo di risorse "non proprie" per svolgere determinate attività.

ACCOUNTABILITY, LA CHIAVE È L'APPROCCIO PROATTIVO

Essere proattivi è il necessario atteggiamento da adottare per non rispondere in futuro di un danno derivante da trattamento dei dati personali attraverso la dimostrazione di aver fatto tutto il possibile per evitarlo.

DIMOSTRARE L'EFFICACIA DELLE MISURE ADOTTATE

Misure organizzative e tecniche rapportate al caso concreto del trattamento ma in grado di essere adatte e adeguate ad una serie sufficientemente ampia di rischi calcolati.

Anticipare le situazioni critiche, gli eventi rischiosi possibili o molto probabili e trovare soluzioni che forniscano un certo margine di sicurezza.

PRISMA @PA

REGISTRO DEI TRATTAMENTI

ARTICOLO 30, CONSIDERANDO 82

OBIETTIVO: fornire un quadro aggiornato dei trattamenti e garantire un trattamento efficiente e sicuro

CONTENUTI:

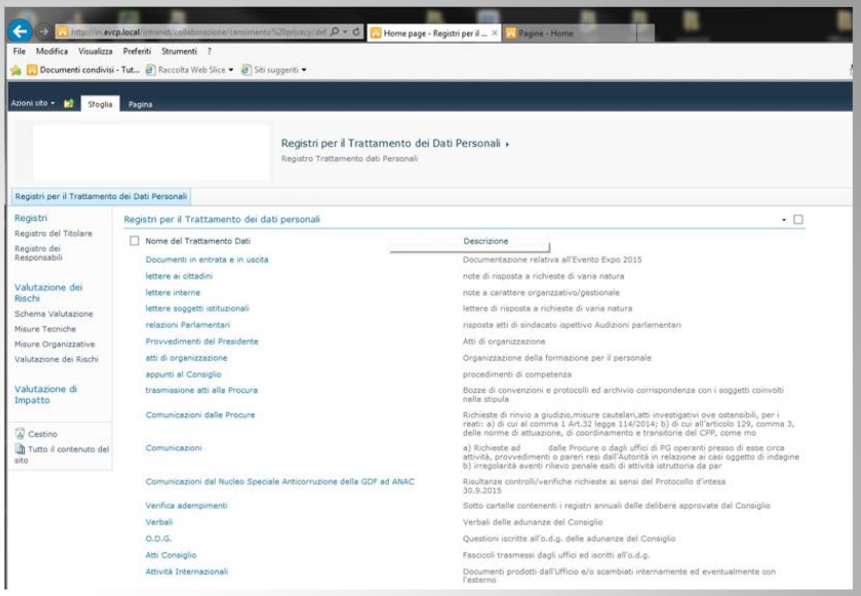
+ Dati del Titolare del trattamento e del DPO
+ Finalità del trattamento;
+ Categorie di interessati, dati personali, destinatari dei dati stessi
+ Termini per la cancellazione
+ Descrizione generale delle misure di sicurezza tecniche e organizzative

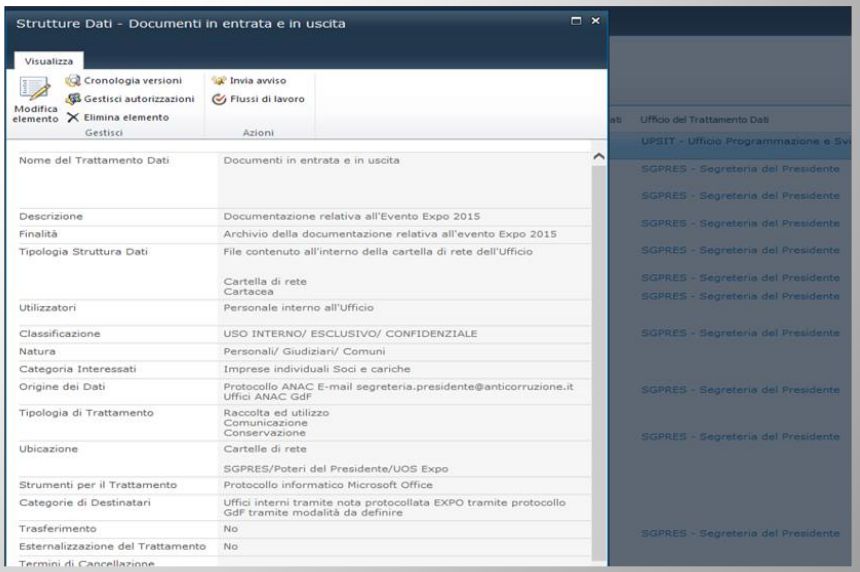
PRINCIPI ISPIRATORI

+ Accountability
+ Minimizzazione
+ Trasparenza
+ Efficacia, efficienza ed economicità

NORME e REGOLAMENTAZIONE

+ Art. 30
+ Considerando 82





PRISMA @PA

CONTESTO: PRISMA E LA P.A.

Eterogeneità della PA

3270445 dipendenti pubblici suddivisi in circa 10.000 PA, più circa 1.000 solo nelle ASL e 44.000 nelle scuole pubbliche

Realtà complessa

13 ecosistemi solo nella PAC

Diffusione sul territorio

Circa 8.000 comuni di cui 5683 piccoli comuni

PRISMA @PA

I contributi espressi in questa presentazione sono da valutare come un punto di vista personale e le eventuali opinioni espresse sono da intendersi opinioni strettamente personali.
E' autorizzato l'uso del materiale presentato a soli fini didattici.

Un ringraziamento speciale per i contributi riguardanti Prisma@PA a: Claudia Trivillino, Monica di Paolo, Piero Flamini e Salvatore Costa.

Fine