REGIONE EMILIA-ROMAGNA
Atti amministrativi
PROTEZIONE CIVILE

Atto del Dirigente DETERMINAZIONE

Num. 315 del 02/02/2022 BOLOGNA

Proposta:	DPC/2022/358 del 01/02/2022
Struttura proponente:	SERV. CONSULENZA GIURIDICA, CONTENZIOSO, CONTROLLI INTERNI AGENZIA REGIONALE PER LA SICUREZZA TERRITORIALE E LA PROTEZIONE CIVILE
Oggetto:	RECEPIMENTO DELLE LINEE GUIDA SULLA PRIVACY BY DESIGN DI CUI ALLA DELIBERAZIONE DI GIUNTA REGIONALE N. 2259/2021
Autorità emanante:	IL DIRETTORE - AGENZIA REGIONALE PER LA SICUREZZA TERRITORIALE E LA PROTEZIONE CIVILE
Firmatario:	RITA NICOLINI in qualità di Direttore
Responsabile del procedimento:	Rita Nicolini

Firmato digitalmente

IL DIRETTORE

VISTE:

- la L.R. 7 febbraio 2005, n. 1 "*Norme in materia di protezione civile e volontariato. Istituzione dell'Agenzia regionale di protezione civile*" e successive modifiche;
- la L.R. 30 luglio 2015, n. 13 "*Riforma del sistema di governo regionale e locale e disposizioni su città metropolitana di Bologna, province, comuni e loro unioni*", con la quale, in coerenza con il dettato della Legge 7 aprile 2014, n. 56, è stato riformato il sistema di governo territoriale e, per quanto qui rileva, è stato ridefinito l'assetto delle competenze dell'Agenzia regionale di protezione civile ridenominata, peraltro, Agenzia regionale per la sicurezza territoriale e la protezione civile, nel seguito "Agenzia regionale";
- la deliberazione di Giunta regionale n. 1023/2015 e la determinazione dirigenziale n. 535/2015 di approvazione del Regolamento di organizzazione e contabilità dell'Agenzia regionale;
- la deliberazione di Giunta regionale n. 622/2016 "*Attuazione seconda fase della riorganizzazione avviata con delibera 2189/2015*";
- la deliberazione di Giunta regionale n. 1770/2020 di "Approvazione riorganizza*zione dell'Agenzia regionale per la sicurezza territoriale e la protezione civile"* di cui alla propria proposta con determinazione n. 3662/2020, a decorrere dal 1° gennaio 2021;

VISTO, altresì il "*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)*" (di seguito Regolamento);

VISTO, in particolare, l'articolo 25 del Regolamento "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*", di seguito riportato:

1. *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;

2. *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.*
3. *Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo;*

VISTA la deliberazione di Giunta regionale n. 2259/2021 con la quale:

- sono stati richiamati il documento "Linee guida 4/2019 del EDPB (European Data Protection Board) sul citato articolo 25 del Regolamento, con particolare riferimento agli obblighi del titolare, ai principi di protezione che abbiano efficacia e all'attuazione di tali principi utilizzando la protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita, nonché il documento di Enisa (European Union Agency for Cybersecurity) del dicembre 2014 "Privacy e protezione dei dati by design – dalla policy all'ingegneria" nel quale Enisa specifica le misure tecnologiche e organizzative da assumere in concreto per dare attuazione ai principi;
- sono state fornite definizioni e indicazioni sui principi in questione nel relativo Allegato "Linee guida sulla privacy by design di Giunta e di Assemblea Legislativa";

- si è disposto di dare attuazione alle misure tecnologiche e organizzative indicando come necessaria la creazione di una check list da pubblicare sul sito Orma, nonché di comunicare ad Enti e Agenzie di cui all'art. 1, comma 3-bis, lett. b) e c), della L. 43/2001 l'adozione della medesima deliberazione, a cui i predetti Enti e Agenzie possono conformarsi con propri atti tenendo conto delle proprie specificità;

RITENUTO di recepire le Linee guida sulla privacy by design, di cui alla citata deliberazione di Giunta regionale n. 2259/2021, in ragione dell'esaustività delle indicazioni ivi riportate e che l'Agenzia regionale adegua, come da allegato 1 alla presente determinazione, al proprio contesto organizzativo in aderenza alla ripartizione delle competenze tra la Direzione e Servizi in tema di attuazione della normativa in materia di protezione dei dati personali, operata con le proprie determinazioni di seguito richiamate:

- n. 1/2019, con le precisazioni di cui alla successiva determinazione n. 890/2019, con cui, nel recepire la DGR n. 1123/2018, sono stati, tra l'altro, individuati i compiti del Direttore quale soggetto attuatore di tale normativa e delegati alcuni di detti compiti ai Responsabili dei Servizi, tra cui quello di adottare soluzioni di "privacy by design e by default";
- n. 687/2021, con la quale la delega dei suddetti compiti è stata confermata in capo ai Responsabili dei Servizi in cui è ora articolata l'Agenzia a seguito del suo recente riassetto organizzativo;

RITENUTO, altresì, di utilizzare, una volta pubblicata nella pagina "Privacy" di ORMA, la citata check list con i relativi aggiornamenti, contenente le misure tecniche ed organizzative per l'attuazione dei principi indicati nelle Linee Guida, da adeguare, ove necessario, al contesto organizzativo dell'Agenzia regionale;

VISTO il decreto legislativo n. 33 del 14/03/2013 "*Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*" e s.m.i.;

VISTE, altresì, le deliberazioni della Giunta regionale:

- n. 2416/2008 "*Indirizzi in ordine alle relazioni organizzative e funzionali tra le strutture e sull'esercizio delle funzioni dirigenziali. Adeguamenti*

conseguenti alla delibera 999/2008. Adeguamento e aggiornamento della delibera 450/2007" e s.m.i;

- n. 468/2017 "*Il sistema dei controlli interni nella Regione Emilia-Romagna*", recepita con determinazioni del Direttore dell'Agenzia regionale n. 700/2018 e n. 2657/2020, e le circolari del Capo di Gabinetto del Presidente della Giunta regionale PG/2017/660476 del 13.10.2017 e PG/2017/779385 del 21.12.2017 concernenti indicazioni procedurali per rendere operativo il sistema dei controlli interni;
- n. 1962/2020 "*Assunzione di un dirigente ai sensi dell'art. 18 della L.R. n. 43/2001 e ss.mm.ii. per il conferimento di incarico di direttore dell'Agenzia regionale per la sicurezza territoriale e la protezione civile*";
- n. 111/2022 recante il Piano triennale di prevenzione della corruzione e della trasparenza 2022-2024, con il relativo allegato D);

RICHIAMATA la L.R. 26 novembre 2001, n. 43, "*Testo unico in materia di organizzazione e di rapporti di lavoro nella Regione Emilia-Romagna*";

ATTESTATO che il sottoscritto dirigente, responsabile del procedimento, non si trova in situazione di conflitto, anche potenziale, di interessi;

ATTESTATA la regolarità amministrativa del presente atto;

DETERMINA

Per le ragioni esplicitate nella parte narrativa

1. di recepire, contestualizzandone le disposizioni alla realtà organizzativa dell'Agenzia regionale per la sicurezza territoriale e la protezione civile, come da Allegato 1, parte integrante e sostanziale del presente atto, le "Linee guida sulla privacy by design" di cui alla deliberazione della Giunta Regionale n. 2259/2021 riguardante i principi della protezione dei dati fin dalla progettazione e della protezione per impostazione predefinita;
2. di trasmettere il presente atto ai Responsabili dei Servizi, anche per darne diffusione a tutti i collaboratori dell'Agenzia regionale;
3. di utilizzare, una volta pubblicata nella pagina "Privacy" di ORMA, la check list, in corso di predisposizione da

parte delle competenti strutture regionali, contenente le misure tecniche ed organizzative per l'attuazione dei principi indicati nelle Linee Guida, da adeguare, ove necessario, al contesto organizzativo dell'Agenzia regionale;

4. di provvedere, sulla base degli indirizzi interpretativi contenuti nella deliberazione della Giunta regionale n. 111/2021, richiamata in parte narrativa, alla pubblicazione del presente atto, ai sensi dell'art. 7-bis, comma 3 del D. Lgs. n. 33/2013 e s.m.i..

Rita Nicolini

ALLEGATO 1

Linee guida sulla Privacy by design

Sommario

Premessa

La digitalizzazione e il progresso tecnologico pongono gli Enti dinanzi ad oneri derivanti dall'etica e dalla normativa in materia di protezione dei dati personali, in particolare per tutelare il diritto alla riservatezza dei cittadini e la capacità degli stessi di esercitare efficacemente i propri diritti di informazione.

È necessario non solo tendere alla conformità alla normativa in materia di protezione dei dati personali ma, in termini sostanziali, adottare un approccio più solido per affrontare la crescita e gli effetti sistemici delle tecnologie dell'informazione e della comunicazione utilizzate su larga scala.

Una tutela piena dei diritti dei cittadini, pure riconosciuti all'art. 8 della Carta dei diritti fondamentali dell'UE, è possibile solo adottando politiche di Privacy by design e by default, da considerare perno cui commisurare il funzionamento e la gestione dei sistemi, lungo l'intero ciclo di vita delle informazioni.

L'Agenzia regionale per la sicurezza territoriale e la protezione civile, di seguito "Agenzia regionale", considera la Privacy by design (d'ora in poi anche solo "PbD") come un concetto suscettibile di trovare applicazione nelle progettazioni di processi, applicativi, infrastrutture verso l'organizzazione, ma soprattuto al di fuori della stessa, verso i propri cittadini.

Il considerando 78 e l'articolo 25 del Regolamento (UE) 2016/679 (di seguito Regolamento) introducono i concetti di protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita, come meglio descritti di seguito:

- **fin dalla progettazione**: il titolare del trattamento deve definire in anticipo rispetto alla gestione concreta del trattamento per quali finalità specifiche, esplicite e legittime i dati personali vengono raccolti e trattati e sempre in anticipo analizzare i possibili rischi per i diritti e le libertà degli interessati;
- **impostazione predefinita**: si riferisce, nell'ambito del trattamento di dati personali, alle scelte compiute rispetto a valori di configurazione od opzioni di trattamento che sono rispettivamente fissati o prescritte in un sistema di trattamento (un'applicazione informativa, un servizio o una periferica o una procedura di trattamento manuale), tali da incidere sulla quantità dei dati personali raccolti, sulla portata del trattamento, sul periodo di conservazione e sull'accessibilità. L'impostazione predefinita deve garantire che siano trattati solo i dati personali necessari per ogni specifica finalità di trattamento.

1. Principi

L'Agenzia regionale riconosce la centralità della Privacy by design quale componente essenziale delle azioni di conformità alla normativa in materia di protezione dei dati personali.

La Privacy by design è considerata dall'Agenzia regionale quale modus operandi predefinito in seno ai processi dell'organizzazione, ivi ricomprendendo i sistemi informativi che supportano l'elaborazione dei dati.

Sono di seguito descritti i sette principi fondamentali della Pbd[1]:

1.1 Proattivo non reattivo; Preventivo non correttivo.

L'approccio orientato al rischio, proprio del Regolamento, determina l'Agenzia regionale ad individuare già nella fase di design i possibili rischi per i diritti e le libertà degli interessati. L'attuazione della PbD comporta l'adozione di misure proattive che anticipino le minacce. Ciò significa identificare i punti di debolezza dei sistema per neutralizzare o ridurre al minimo i rischi ed è certamente più auspicabile che applicare rimedi e misure per risolvere gli incidenti di sicurezza (anche nel caso che sia un data breach) una volta che si sono verificati.

Da ciò deriva che, in aderenza alla ripartizione di competenze di cui alla determinazione del Direttore dell'Agenzia regionale n. 1/2019, con le precisazioni di cui alla determinazione n. 890/2019, di recepimento della deliberazione di Giunta regionale n. 1123/2018 e alla determinazione n. 687/2021, il Direttore, in qualità di Soggetto Attuatore e i Responsabili dei Servizi, quali soggetti delegati, cui competono attribuzioni in tema di attuazione della normativa in materia di protezione dei dati personali, devono implementare sin dal principio metodi sistematici di analisi di processi, trattamenti e tecnologie, al fine di prevenire gli aspetti patologici delle criticità di Privacy e sicurezza informatica rilevate sin da principio.

1.2 Privacy per impostazione predefinita

La PbD assicura agli utenti i più alti livelli di Privacy, misurati dal contesto dell'organizzazione e dallo stato dell'arte, disponendo che i dati personali siano automaticamente protetti in qualsiasi sistema, applicazione, prodotto o servizio.

In questo caso rimandare alla misurazione dello **stato dell'arte** significa che i titolari hanno l'obbligo di tenere conto degli attuali progressi compiuti dalla tecnologia, implicando un continuo aggiornamento.

Tale requisito, in termini pratici, è un richiamo conclamato al **principio della minimizzazione** da applicarsi a tutte le fasi e le operazioni del trattamento (raccolta, elaborazione, conservazione ecc.).

Si rende, pertanto, necessario:

- definire i criteri di raccolta dei dati nella maniera più rigorosa possibile;

---

1 Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada. Privacy by Design: The 7 Foundational Principles, Jan 2011 https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf; Ann Cavoukian, Ph.D. Information & Privacy Commissioner Ontario, Canada. Operationalizing Privacy by Design. A guide to implementing strong Privacy practices, Dec 2012 http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf.

- limitare l'uso dei dati personali alle finalità per le quali sono raccolti, fatto salvo il Considerando 50, art. 5 par. 1 lett. a), art. 6 par. 4 del Regolamento per i quali sono stati raccolti;
- verificare sin da subito l'assolvimento delle condizioni di liceità del trattamento;
- limitare l'accesso ai dati personali alle parti coinvolte nel trattamento in aderenza al principio del "need to know" e creando profili di accesso differenziati;
- definire rigorosi limiti di tempo per la conservazione, in aderenza alle prescrizioni di legge e al manuale della conservazione.

1.3 Privacy integrata nel design

La Privacy deve essere parte integrante e inscindibile dei sistemi, delle applicazioni, dei prodotti e servizi, nonché dei processi dell'Agenzia regionale.

Non può essere considerato un livello o un modulo aggiuntivo che si aggiunge a un'entità preesistente, ed anzi deve essere integrato tra i requisiti nelle fasi di sviluppo e progettazione stessi.

Per garantire che la Privacy sia presa in considerazione nelle prime fasi di progettazione, il Direttore dell'Agenzia regionale e i Responsabili dei Servizi tti Attuatori, devono:

- considerare la protezione dei dati personali come un requisito essenziale all'interno del ciclo di vita dei sistemi e servizi, nonché nella progettazione dei processi organizzativi;
- eseguire un'analisi dei rischi dei diritti e delle libertà delle persone e, quando applicabile, eseguire valutazioni d'impatto sulla protezione dei dati, come parte integrante di ogni nuova iniziativa di trattamento;
- documentare tutte le decisioni adottate all'interno dell'organizzazione nella prospettiva del " Privacy design thinking";
- richiedere parere al DPO (Data Protection Officer) quando le operazioni sopra indicate presentino criticità di rilievo.

1.4 Massima funzionalità: valore positivo e non valore zero

Tale principio assolve all'onere di soddisfare tutti gli interessi e gli obiettivi dell'Agenzia regionale, rappresentando che non necessariamente è imposto scegliere a vantaggio di una singola posizione ed escluderne un'altra, come nel caso della relazione tra Privacy e sicurezza o Privacy e usabilità. L'Agenzia regionale deve porsi l'obiettivo di trovare un equilibrio, assumendo che possano coesistere interessi diversi e legittimi, come quelli dell'organizzazione e degli utenti cui è rivolto il servizio; disponendo, altresì, efficaci canali di comunicazione e partecipazione che, in alcuni casi, possano anche ricomprendere contributi promananti direttamente dagli interessati.

1.5 Sicurezza end-to-end: protezione completa del ciclo di vita

La Privacy va garantita per tutto il ciclo di vita dei dati, ovvero deve essere assicurata la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi che elaborano i dati, deve

essere assicurata trasparenza e capacità d'intervento sui dati e dovrebbero essere attuate le misure più adeguate al rischio correlato al trattamento quali:

- tecniche di pseudonimizzazione;
- meccanismi di coerenza tra classificazione dei dati e delle informazioni e accesso agli stessi;
- crittografia per impostazione predefinita;
- la distruzione sicura e garantita delle informazioni a fine ciclo.

1.6 Visibilità e trasparenza

Come riportato dall'art. 25 del Regolamento, l'Agenzia regionale deve essere in grado di dimostrare la conformità della propria organizzazione allo stesso. Anche elevati livelli di trasparenza consentono all'Agenzia regionale di rappresentare al propria diligenza sia dinanzi all'Autorità garante sia nei confronti degli interessati.

Devono essere considerati puntualmente i seguenti aspetti:

- Nelle informative per il trattamento dei dati personali e nella documentazione pubblicata devono essere riportate informazioni chiare e comprensibili agli utenti consentendo agli interessati di comprendere gli ambiti di trattamento dei loro dati, i rischi a cui possono essere esposti e come esercitare i propri diritti in materia di protezione dei dati.
- Condividere i dettagli di contatto del responsabile del trattamento dei dati dell'organizzazione;.
- Stabilire per i soggetti interessati meccanismi di comunicazione accessibili, semplici ed efficaci.

1.7 Rispetto per la Privacy dell'utente: centralità dell'interessato

Le azioni di Privacy by design richiedono che l'interessato (e quindi l'individuo), sia al centro, e, pertanto, ogni misura adottata deve concentrarsi verso la garanzia della loro Privacy.

L'Agenzia regionale deve, pertanto, assicurare la protezione dell'utente indipendentemente dalla sua partecipazione spontanea, ma con opzioni che la rendono in un certo senso obbligatoria.

In ragione del fatto che l'Agenzia regionale, in linea generale, effettua trattamenti di dati personali al fine di adempiere ad un obbligo di legge, o per l'esercizio esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito l'Agenzia regionale stessa, e, in ogni caso, in aderenza a quanto disposto dall'art. 2ter e 2sexies del Codice per la protezione dei dati personali, si rende necessario progettare processi, applicazioni, prodotti e servizi incentrati sul garantire la riservatezza degli interessati, proprio in ragione della non necessaria consultazione dell'utente.

2. REQUISITI DI PRIVACY DEI SISTEMI

La progettazione di sistemi sicuri risponde certamente agli esiti dell'analisi dei rischi correlati al trattamento, tenendo in debita considerazione le minacce a riservatezza, integrità e disponibilità dei dati.

Sussistono, tuttavia, diversi fattori di rischio che, per una piena conformità del trattamento, devono essere certamente considerati, quali la perdita di controllo nel processo decisionale, la raccolta eccessiva di dati, la reidentificazione, la discriminazione delle persone, i pregiudizi nelle decisioni automatizzate, la mancata comprensione dei trattamenti da parte degli utenti e i rischi di trattamento illecito o di profilazione invasiva o non corretta, sono esempi di rischi per la Privacy che hanno un chiaro effetto sui diritti e sulle libertà delle persone che non possono essere gestiti utilizzando solo un modello di rischio tradizionale che si concentra esclusivamente sugli obiettivi di sicurezza.

A tal fine l'analisi del rischio deve ricomprendere ulteriori tre obiettivi di protezione dei dati personali:

- NON COLLEGABILITA': ovvero i dati personali elaborati all'interno di un dominio non dovrebbero essere collegati ai dati personali in un dominio diverso. Si tratta di una misura atta a ridurre fortemente il rischio di un utilizzo non autorizzato dei dati personali, nonché la creazione di profili a mezzo dell'interconnessione di dati provenienti da insiemi diversi.
- TRASPARENZA: ovvero l'Agenzia regionale deve rendere chiari e intellegibili agli interessati gli elementi essenziali del trattamento. Tali informazioni devono, in ogni caso, essere conosciute e condivise da tutte le parti coinvolte, ivi compresi gli operatori dell'Agenzia regionale che definiscono il trattamento.
- CONTROLLO: ovvero è necessario garantire la possibilità per le parti coinvolte nel trattamento dei dati personali, e in particolare i soggetti i cui dati sono trattati, di intervenire nel trattamento ogniqualvolta sia necessario per applicare misure correttive al trattamento delle informazioni. Tale obiettivo è strettamente connesso alla definizione e attuazione delle procedure per l'esercizio dei diritti in materia di protezione dei dati che l'Agenzia regionale ha già adottato.

2.1 Privacy Engineering

Per Privacy Enginenering s'intende un processo sistematico con un focus orientato al rischio che ha l'obiettivo di tradurre, in termini pratici e operativi, i principi della Privacy by design nel ciclo di vita dei sistemi informativi attraverso il quale sono trattati dati personali.

Al fine di rendere la Privacy parte integrante della progettazione del sistema, già nelle fasi iniziali di sviluppo del concetto del sistema e dell'analisi dei suoi requisiti, è necessario implementare **strategie di Privacy by design**. Le strategie fungono da ponte tra l'elaborazione dei principi imposti dalla legge e l'attuazione della Privacy in soluzioni concrete. Le strategie quindi possono essere definite come degli approcci fondamentali per raggiungere dei determinati obiettivi di progettazione.

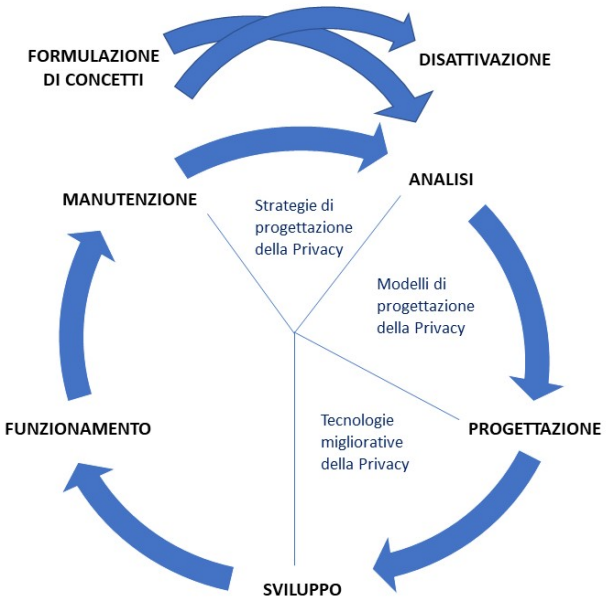
Ad un livello più basso di analisi, devono poi essere considerati dei **modelli di Privacy (Privacy design patterns)**, ovvero modelli atti a delineare le componenti del software e le loro relazioni: perfezionano l'architettura del sistema permettendo di raggiungere determinati requisiti funzionali (sono comunque sottoposti ad alcuni vincoli strutturali). L'obiettivo di questi modelli è creare un catalogo di soluzioni riutilizzabili nella progettazione della Privacy dei sistemi, anche al fine di standardizzare il processo di progettazione.

Infine, nella fase di sviluppo vero e proprio, debbono essere utilizzate le cosìddette **PETS (Privacy Enhancing Technologies)** volte all'implementazione concreta dei modelli di progettazione della Privacy.

Più spcificatamente per PET intendiamo "un sistema coerente di misure ICT volto a proteggere la Privacy eliminando o riducendo i dati personali o impedendo il trattamento non necessario e/o indesiderato dei dati personali, il tutto senza perdere la funzionalità del sistema informativo"[2].

D'altra parte l'individuazione della design strategy, design pattern e PETs richiama la divisione del processo decisionale in una fase strategica (spiegando cosa bisogna ottenere), una tattica (rendendo più concreti gli obiettivi, anche dal punto di vista organizzativo) e una operativa (implementando la fase tattica attraverso l'allocazione di risorse, ecc.) che si ritrova nella letteratura del management.

Di seguito viene rappresentata la connessione tra le fasi di sviluppo di un sistema e gli elementi essenziali della Privacy by design prima descritti:



2 COM (2007) 228 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on promoting data protection by Privacy Enhancing Technologies (PETs) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0228&from=EN.

2.1.1 Le strategie di Privacy by design

La dottrina più autorevole individua otto diverse strategie di Privacy by design note come: "minimizzare", "nascondere", "separare", "aggregare", "informare", "controllare", "applicare" e "dimostrare".

A loro volta, queste otto strategie possono essere suddivise in due categorie: l'una orientata ai dati, detta data-oriented (minimizzare, nascondere, separare, aggregare) e l'altra orientata ai trattamenti, detta process-oriented (informare, controllare, applicare e dimostrare).

Queste strategie non sono separate ed esclusive. **Le loro caratteristiche possono essere applicate parallelamente durante la progettazione di un sistema IT**, il quale può essere inteso sia come database (fanno parte di questa categoria, per esempio, i social network e i sistemi di amministrazione governativi) sia come sistema di flusso di informazioni (information flow system: questi sistemi si basano sull'enorme quantità di dati che viene prodotta e processata oggigiorno, riferendosi anche ai Big Data).

Queste strategie, inoltre, sono state approfondite e arricchite con quelle che vengono definite "**tattiche"**, ovvero delle tattiche volte a facilitare l'implementazione delle otto strategie per ottenere un livello di protezione della Privacy qualitativamente più elevato. **Una tattica è un approccio**, coerente con i principi di Privacy by design, **che contribuisce al raggiungimento di una Privacy design strategy globale.**

1) Minimizzare (Minimize)

L'obiettivo di questa strategia è raccogliere ed elaborare la minor quantità di dati possibile, scongiurando così il trattamento di dati non necessari e limitando i possibili impatti sulla privacy. Ciò può essere ottenuto raccogliendo dati da un numero inferiore di soggetti (riducendo la dimensione della popolazione) o meno dati da soggetti (riducendo il volume delle informazioni raccolte), per i quali possono essere utilizzate le seguenti tattiche:

- Escludere (Exclude): escludere a priori soggetti e attributi irrilevanti per il trattamento. Sono escluse quante più informazioni possibili, a meno che la loro inclusione non possa essere giustificata come assolutamente necessaria per la finalità prefissata.
- Selezionare (Select): selezionare solo il campione di individui rilevanti e gli attributi richiesti, con un approccio conservativo nello stabilire i criteri di selezione ed elaborare solo i dati che soddisfano i criteri di selezione (white list)
- Rimuovere (Strip): eliminare parzialmente i dati personali non appena cessano di essere necessari, il che richiede di stabilire preventivamente il periodo di conservazione di ciascuno dei dati raccolti e di istituire meccanismi di cancellazione automatica al termine di tale periodo. Nel caso in cui i dati facciano parte di un record che contiene più informazioni del necessario, il valore dei campi non necessari può essere modificato in un valore predefinito prefissato.
- Eliminare (Destroy): eliminare completamente i dati personali non più necessari.

2) Nascondere (Hide)

Questa strategia si concentra sulla limitazione dell'accesso ai dati stabilendo i mezzi idonei a garantire la protezione della riservatezza dei dati personali e le loro connessioni e può essere implementata attraverso vari design patterns: l'utilizzo di profilazioni individuali, l'utilizzo di dati criptati, pseudonimizzazione, anonimizzazione, l'utilizzo di mix networks (per nascondere dei modelli ricorrenti di traffico) e altre tecniche per impedire l'associazione tra i dati.

In particolare:

L'anonimizzazione permette di proteggere e nascondere l'identità di un soggetto rendendo anonimi i dati: ogni informazione che possa servire da elemento identificatore viene rimossa dai dati.

Nella **pseudonimizzazione**, invece, i dati personali vengono trattati in modo che non possano essere riferiti ad un individuo senza l'utilizzo di informazioni aggiuntive, le quali devono essere conservate separatamente e devono essere protette da misure che assicurino che un set di dati non vengano associati all'identità di un individuo.

Sintetizzando, questa strategia cerca di prevenire il più possibile l'esposizione dei dati combinando, offuscando, dissociando o limitando l'accesso ad ogni deposito, condivisione o operazione che concerne i dati personali, entro i limiti della finalità perseguita.

Le tattiche che possono essere utilizzate sono:

- Limitare (Restrict): limitare l'accesso ai dati personali ponendo dei limiti attraverso una politica di controllo degli accessi che attui il principio del "need to know"
- Combinare (Mix): raggruppare informazioni sugli interessati utilizzando tecniche di generalizzazione e soppressione per evitare correlazioni.
- Offuscare (Obfuscate): rendere inintelligibili i dati personali per coloro che non sono autorizzati a consultarli, mediante tecniche di crittografia e hashing, sia per operazioni di conservazione che di trasmissione di informazioni.
- Dissociare (Dissociate): eliminare il collegamento tra set di dati che dovrebbero essere mantenuti indipendenti, nonché gli attributi di identificazione dei record di dati per evitare correlazioni tra di essi, con particolare attenzione ai metadati.

3) Separare (Separate)

L'obiettivo di questa strategia è evitare, o almeno ridurre al minimo il rischio che durante il trattamento, all'interno dell'Agenzia regionale, diversi dati personali dello stesso individuo utilizzati in processi indipendenti possano essere combinati per creare un profilo completo dell'interessato. Per questo è necessario mantenere contesti di elaborazione indipendenti che rendano difficile correlare dataset che dovrebbero essere scollegati. Questa strategia è fortemente collegata a quella del nascondere i dati (hide) e le tattiche che possono essere usate per implementarla sono:

- Distribuire (Distribute): eseguire una partizione dei dati personali in modo tale che sia necessario un ulteriore accesso per elaborarli.

- Isolare (Isolate): utilizzare sistemi e applicazioni diversi per implementare architetture decentralizzate e distribuite che elaborano le informazioni distintamente

4) Aggregare (Abstract)

I dati personali dovrebbero essere elaborati raggiungendo il più alto livello di aggregazione possibile, mantenendo il dettaglio al minimo necessario con riferimento alla finalità del trattamento.

L'aggregazione dei dati in gruppi di attributi o di persone riduce la quantità di informazioni dettagliate che vengono utilizzate, e riduce l'impatto di eventuali violazioni o usi illeciti.

Questa strategia comprende le seguenti tattiche:

- Sintetizzare (Summarize): generalizzare i valori degli attributi utilizzando range o intervalli di valori;
- Raggruppare (Group): aggregare le informazioni di un gruppo di record in categorie anziché utilizzare le informazioni di dettaglio su ciascuno dei soggetti che appartengono al gruppo, utilizzando valori medi o generali;
- Alterare: utilizzare valori approssimativi o modificare i dati reali utilizzando un tipo di "rumore casuale" invece di utilizzare il valore esatto dei dati personali.

5) Informare (Inform)

Questa strategia è impostata sul concetto di trasparenza: l'interessato dovrebbe essere informato in maniera adeguata ogniqualvolta vengono trattati i dati personali che lo riguardano. L'informativa di cui agli artt. 13 e 14 del Regolamento è lo strumento attraverso cui dare attuazione a tale principio. All'interessato devono essere fornite informazioni riguardanti l'identità e i dati di contatto del titolare, i dati di contatto del DPO, la natura dei dati che vengono processati, le finalità e la base giuridica del trattamento. I soggetti a cui si riferiscono i dati dovrebbero essere informati anche nel caso i propri dati vengano condivisi con terzi e devono essere informati anche su quali sono i loro diritti e su come esercitarli.

Le tattiche disponibili sono:

- Fornire (Supply): fornire agli interessati tutte le informazioni indicate dal Regolamento tra cui: quali dati personali vengono trattati, come vengono trattati e le finalità sottese al trattamento.Dovrebbe essere indicato anche chi può essere contattato dagli interessati e come, per porre domande inerenti il trattamento ed esercitare i diritti ad essi riconosciuti dalla normativa.
- Notificare (Notify): informare gli interessati del trattamento quando i dati non sono raccolti direttamente da loro, nel momento in cui questi sono stati ottenuti ed entro un massimo di un mese, oppure, se saranno utilizzati per comunicazioni con loro, nel primo messaggio. I soggetti devono essere informati anche se i loro dati saranno ceduti a terzi. Devono inoltre essere attuati meccanismi di segnalazione ai soggetti i cui dati personali hanno subito delle violazioni della sicurezza che possono essersi verificate e possono comportare un grave rischio per le loro libertà

e diritti, utilizzando un linguaggio chiaro e semplice per descrivere la natura della violazione.

- Spiegare (Explain): fornire informazioni sul trattamento dei dati in modo conciso, trasparente, intelligibile e facilmente accessibile con un linguaggio chiaro e semplice. Per evitare politiche informative dense e complesse vale la pena adottare un approccio a strati che fornisca in primo luogo le informazioni di base e renda disponibili ulteriori informazioni dettagliate a un secondo livello.

6) Controllare (Control)

Gli interessati (vale a dire i soggetti a cui si riferiscono i dati personali) dovrebbero essere messi nelle condizioni di esercitare un certo grado di controllo in ordine al trattamento dei propri dati personali. Questa strategia è fortemente collegata alla precedente, quella sull'informazione. Come richiesto dagli articoli 15-19 del Regolamento deve essere garantito all'interessato il diritto di accedere, rettificare, limitare o cancellare (diritto all'oblio) i dati personali che lo riguardano.

Questa strategia comprende le tattiche di[3]:

- Alert (alert): informare l'utente in tempo reale quando vengono raccolti dati personali
- Scegliere (Choose): consentire la selezione o l'esclusione dei dati personali da qualsiasi elaborazione, parzialmente o interamente.
- Aggiornare (Update): fornire agli interessati modalità per mantenere i propri dati precisi, corretti, e aggiornati.
- Ritirare (Retract): consentire il diritto dell'interessato alla rimozione completa, e tempestiva, dei dati che lo riguardano (diritto all'oblio, articolo 17 del DGPR).

7) Applicare (Enforce)

Questa strategia garantisce che il trattamento dei dati personali sia compatibile e rispetti i requisiti di liceità imposti dal Regolamento. Per questo, è necessario definire un quadro di policy in materia di privacy, supportate dalle figure apicali dell'organizzazione, e un modello organizzativo che definisca ruoli e le responsabilità in termini di attuazione della normativa. La cultura della privacy deve essere una parte essenziale dell'organizzazione . Le seguenti tattiche possono aiutare a raggiungere questo obiettivo:

- Creare (Create): riconoscere il valore della Privacy e definire policies e procedure che consentano all'Agenzia regionale di essere conformi alla normativa in materia di protezione dei dati personali. È inoltre necessario sviluppare un piano di formazione e sensibilizzazione per tutti i membri dell'organizzazione, al fine di garantire consapevolezza e partecipazione.
- Mantenere (Mantain): le policies e le procedure che definiscono le misure tecniche ed organizzative individuate in attuazione della normativa devono essere mantenute aggiornate e verificate da parte dell'Agenzia regionale.

3 La dottrina maggioritaria individua tra le tattiche di tale strategia anche il "consenso" che, tuttavia, l'Entem in aderenza al Considerando 43 del Regolamento e delle Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679 dell'EDPB ritiene di non sviluppare.

- Sostenere (Uphold): deve essere assicurata la conformità, l'efficacia e l'efficienza delle policies e delle procedure, così come delle misure e dei controlli che sono implementati dall'Agenzia regionale in attuazione della normativa in materia di protezione dei dati personali.

8) Dimostrare (Demonstrate)

L'Agenzia regionale deve essere in grado di dimostrare, come indicato dall'art. 24 del Regolamento, la compliance con il quadro normativo in materia di protezione dei dati personali. Pertanto, non solo si deve rispettare la disciplina esistente, ma l'Agenzia regionale deve poter dimostrare tale conformità. E' necessario, quindi, acquisire le evidenze delle valutazioni espresse dall'Agenzia regionale nelle determinazioni in materia di protezione dei dati personali.

Questa strategia comprende le tattiche di:

- Registrare (Record): è necessario documentare ogni decisione assunta dall'Agenzia regionale in materia di protezione dei dati personali.
- Verificare (Audit): è necessario effettuare una revisione sistematica e documentata della conformità delle policies e delle procedure in materia di protezione dei dati personali.
- Rendicontare (Report): è necessario documentare gli esiti degli audit, delle valutazioni d'impatto, delle violazioni dei dati personali e ogni altra operazione rilevante e metterli a disposizione dell'autorità di controllo ove richiesto. [4].

Di seguito si riporta la tabella riassuntiva delle strategie di Privacy by design e relative tattiche:

Strategie di Privacy by design	Tattiche
MINIMIZZARE	Escludere
	Selezionare
	Segmentare
	Cancellare
NASCONDERE	Limitare
	Combinare
	Offuscare

4 Cfr. COLESKY M., HILLEN C., HOEPMAN J.-H., A Critical Analysis of Privacy Design Strategies, in "Security and Privacy Workshops (SPW)", IEEE, 2016, pp. 33–38, DOI: 10.1109/SPW.2016.23.

	Dissociare
SEPARARE	Distribuire
	Isolare
AGGREGARE	Sintetizzare
	Raggruppare
INFORMARE	Fornire
	Notificare
	Spiegare
CONTROLLARE	Scegliere
	Aggiornare
	Ritirare
APPLICARE	Creare
	Mantenere
	Sostenere
DIMOSTRARE	Registrare
	Verificare
	Rendicontare

2.1.2 Modelli di Privacy by design

Vi sono molte raccolte o cataloghi di “modelli” di Privacy by design in cui possono essere trovare obiettivi e informazioni su come utilizzarli. A titolo esemplificativo si riportano

a) PRIPARE (Preparare l'Industria alla Privacy by design supportandone l'Applicazione nella Ricerca) è un progetto finanziato dall'Unione Europea in cui è stato sviluppato un catalogo di 26 Privacy design patterns[5]

5 Online - privacypatterns.eu - collecting patterns for better privacy https://privacypatterns.eu/.

b) repository interattivo di soluzioni che classifica 40 modelli di progettazione della Privacy secondo gli 11 principi di protezione definiti da la norma ISO/IEC 29100:2011 predisposto dall'Università di Economia e Commercio di Vienna
c) Iniziativa propria di diverse università https://privacypatterns.org/ in cui si propone un catalogo di modelli al fine di standardizzare il linguaggio per le tecnologie di PbD, documentare soluzioni ai comuni problemi di Privacy, fornire ausilio agli sviluppatori nella soluzione ai requisiti Privacy.

2.1.3 PETs

Definite le strategie ed i modelli di PbD questi devono essere implementati in fase di sviluppo del sistema utilizzando specifiche soluzioni tecnologiche.

In ragione del contesto tecnologico sempre in evoluzione, l'efficacia di tali tecnologie muta nel tempo e, pertanto, si rinvia alla specifica definizione di queste che la struttura competente in materia di protezione dei dati personali e sicurezza informatica produce in un elenco/checklist che condivide nell'intranet aziendale.