STRUMENTI A SUPPORTO DELLE AZIENDE PER L'ATTUAZIONE DEL GDPR E LA MITIGAZIONE DEI RISCHI

Dott.ssa Simona Montinari
Product Manager Kiwa Cermet

Unione Province d'Italia
UPI
Emilia-Romagna

PNT
CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

idea
Kiwa Cermet Idea

ARGOMENTI

- ✓ Lo Scenario di riferimento
- ✓ Lo stato di adeguamento del GDPR in Italia
- ✓ La norma UNI/PDR 43:2018
- ✓ Altri strumenti per la mitigazione dei rischi in ambito GDPR
- ✓ Lo scenario in evoluzione

LO SCENARIO DI RIFERIMENTO

Il 2018 è stato un anno cruciale per la data protection:

- Entrata in vigore del GDPR il 25 maggio in UE.
- Maggiore consapevolezza della pubblica opinione della relazione tra la protezione dei dati personali e le libertà e diritti degli interessati.
- Molteplici casi di «incidenti» relativi alla protezione dei Dati (ad es. caso di Cambridge Analytica con calo valore borsistico di Facebook) in cui il nodo centrale non era legato alla sicurezza dei dati personali.

LO SCENARIO DI RIFERIMENTO (2)

- Un trattamento illecito di dati personali non è tollerato dall'opinione pubblica.
- Può portare a conseguenze rilevanti per la democrazia del paese più potente del mondo.
- L'UE ha consolidato la sua leadership con il GDPR.
- In Italia gran parte delle imprese hanno reagito al GDPR investendo.

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA

- Dal 25 maggio 2018 l'attenzione verso la tutela dei dati personali si è innalzata, con l'obiettivo di favorire la crescita della fiducia dei cittadini europei nell'economia e nella società digitale.

- Per contro gli attacchi informatici non danno tregua alle organizzazioni.

- Le aziende italiane hanno incrementato la spesa in soluzioni tecnologiche legate alla protezione dei dati e stanno investendo nella sensibilizzazione dei propri dipendenti.

A che punto siamo?

Unione Province d'Italia UPI Emilia-Romagna
CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

500 giorni di GDPR

Cosa è cambiato nel mondo della protezione dei dati personali?

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (2)

Figura 1 - *Il percorso di adeguamento al GDPR – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

- *Il 59% delle organizzazioni hanno in corso un progetto di adeguamento al GDPR.*
- *Un quarto delle aziende si è dichiarata conforme al GDPR.*
- *Solo l'8% delle aziende si trova ancora nella fase di definizione dei requisiti.*

Unione Province d'Italia UPI Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

idea Kiwa Cermet Idea

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (3)

Figura 2 - *Il percorso di adeguamento al GDPR per settore di mercato – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

- *Per il settore bancario il percorso di adeguamento sembra essere ben tracciato.*
- *Il settore manifatturiero ha avuto una % di crescita maggiore (dal 42% all'87%).*
- *Anche utility e GDO hanno percentuali elevate.*
- *Il mondo assicurativo sembra essere in ritardo, con il 57% di aziende che dichiarano avere in corso un progetto sul GDPR.*

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (4)

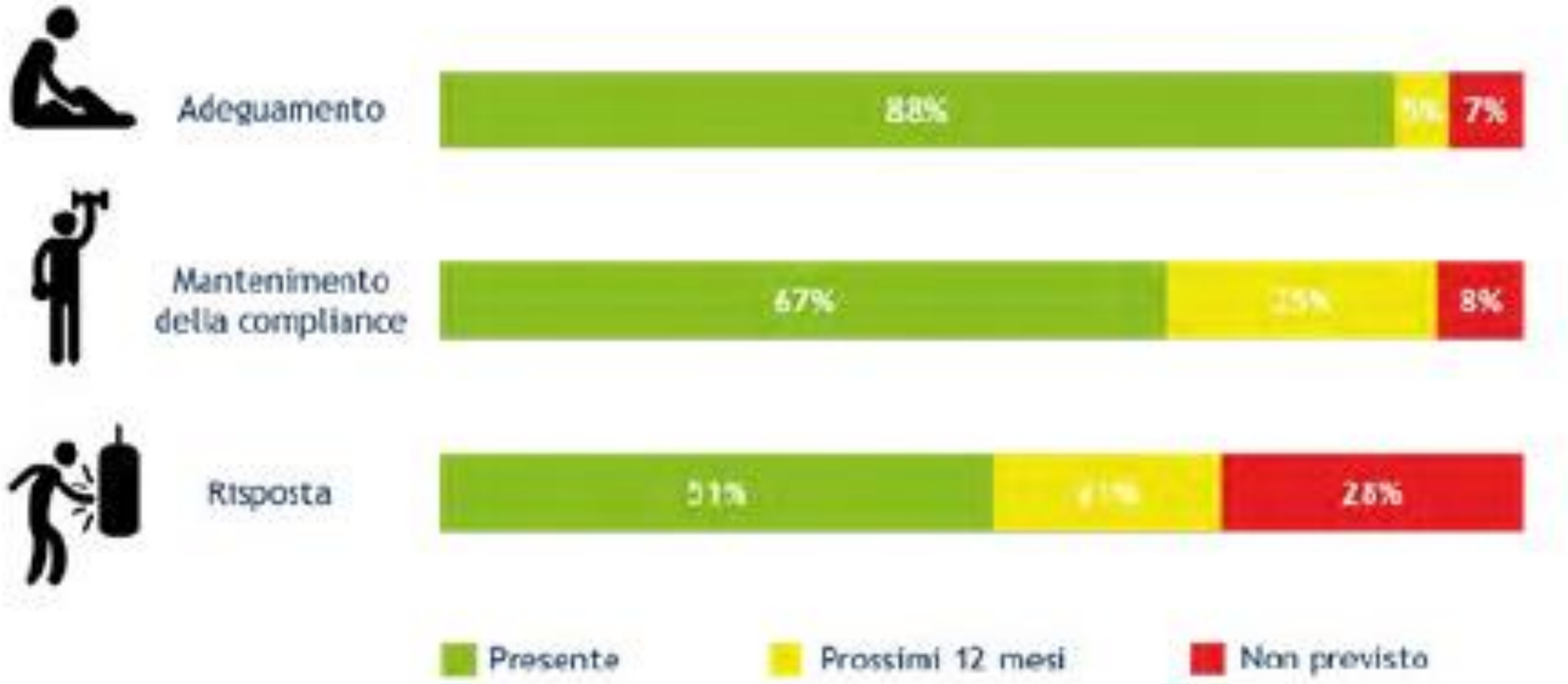


Figura 3 - *Il budget dedicato al GDPR – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

- *Nel 2018 notevole incremento di budget dedicato alle misure di adeguamento al GDPR rispetto al 2017 (dal 58% all'88%).*
- *Minore la % di aziende che dichiarano un budget dedicato a misure di risposta agli eventi di sicurezza che potrebbero verificarsi (data breach).*

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (5)

Figura 4 - *Il budget dedicato a misure di adeguamento al GDPR per settore di mercato – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

- *Da notare che ben il 12% delle aziende del settore retail e GDO ha dichiarato l'assenza del budget per l'adeguamento al GDPR e l'intenzione di non prevederlo in futuro.*
- *Per i settori bancario e assicurativo il budget copre in pratica tutte le attività.*

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (6)

Le principali azioni già implementate:

- ❑ Creazione del registro dei trattamenti (85%)
- ❑ Individuazione ruoli e responsabilità (81%)
- ❑ Raccolta e mappatura dei dati (78%)
- ❑ Modifica della modulistica (76%)
- ❑ Procedura di data breach notification (68%)
- ❑ Definizione delle politiche di sicurezza e valutazione dei rischi (66%)
- ❑ Valutazione d'impatto sulla protezione dei dati personali (56%)
- ❑ Implementazione processi per l'esercizio dei diritti dell'interessato (54%)
- ❑ Revisione contrattualistica con i fornitori di servizi tecnologici (48%)

Unione Province d'Italia UPI Emilia-Romagna
CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

500 giorni di GDPR

Cosa è cambiato nel mondo della protezione dei dati personali?

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (7)

Figura 5 - *Le principali criticità riscontrate – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Unione Province d'Italia UPI Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

idea Kiwa Cermet Idea

500 giorni di GDPR

Cosa è cambiato nel mondo della protezione dei dati personali?

LO STATO DI ADEGUAMENTO AL GDPR IN ITALIA (8)

Figura 7 - *La presenza del DPO per settore di mercato – Fonte: Osservatorio Information Security & Privacy, School of Management Politecnico di Milano*

Unione Province d'Italia UPI Emilia-Romagna

CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

idea Kiwa Cermet Idea

L'ATTIVITÀ ISPETTIVA DEL GARANTE

Privacy: indagine in 18 Paesi, carenze per imprese e enti pubblici

(AGI) - Roma, 5 mar. – Si è svolta una indagine a tappeto ("sweep") in 18 Paesi (Italia inclusa) a cura delle Autorità di protezione dati appartenenti al *Global Privacy Enforcement Network (GPEN)* **per verificare il rispetto del principio di accountability in Europa ai sensi del nuovo Regolamento**.

L'ATTIVITÀ ISPETTIVA DEL GARANTE (2)

RISULTATI ITALIANI - L'indagine ha coinvolto **19 soggetti pubblici (Regioni e Province autonome) e 54 società *in-house*.**
Viene giudicata «Molto grave» la gestione della valutazione dei rischi:

- ✓ il **24% delle società in-house e il 58% delle Regioni** non hanno processi documentati per la «valutazione dei rischi» sulla protezione dei dati personali, in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.
- ✓ ***il 20%* delle Regioni non tiene traccia** neanche dei dati personali comunicati o trasmessi a terzi.

L'ATTIVITÀ ISPETTIVA DEL GARANTE (3)

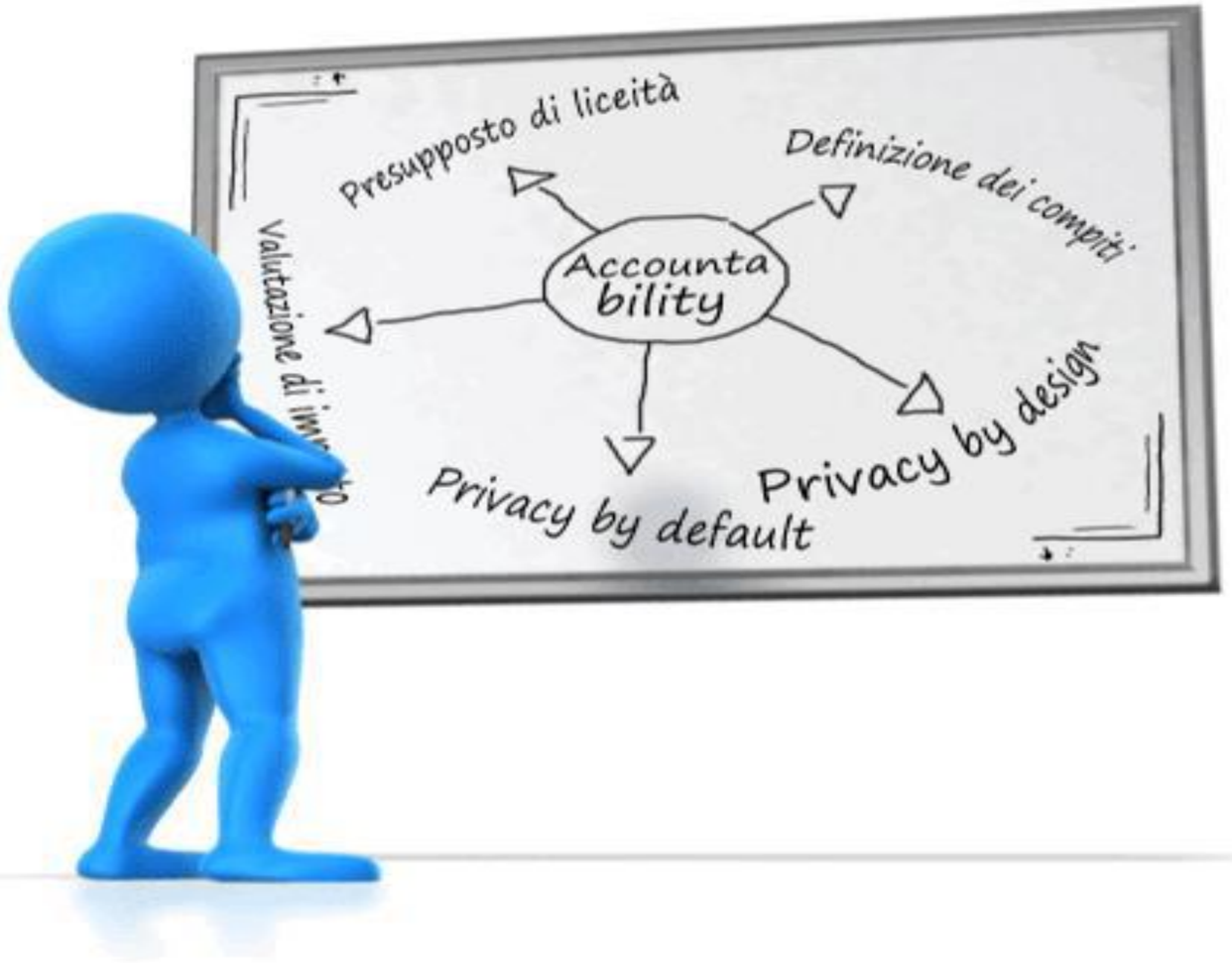
Viene giudicata «grave» la gestione delle richieste e dei reclami:

- ✓ **il 48% delle Regioni e il 24% delle società non hanno policy e procedure per la gestione delle richieste e dei reclami da parte degli interessati o delle stesse Autorità**;
- ✓ **Viene giudicata «carente» la gestione degli incidenti di sicurezza (Data Breach):**
  - **il 20% delle organizzazioni non ha ancora implementato una procedura di risposta agli incidenti di sicurezza** che includa, tra l'altro, la notifica all'Autorità e, in caso di alto rischio per le libertà e i diritti degli interessati, anche la comunicazione a questi ultimi".
  - **Il 25% delle organizzazioni non dispone di un registro per documentare le violazioni subite.**

500 giorni di GDPR

Cosa è cambiato nel mondo della protezione dei dati personali?

NECESSITÀ DI UN APPROCCIO SISTEMICO



Unione Province d'Italia
UPI Emilia-Romagna

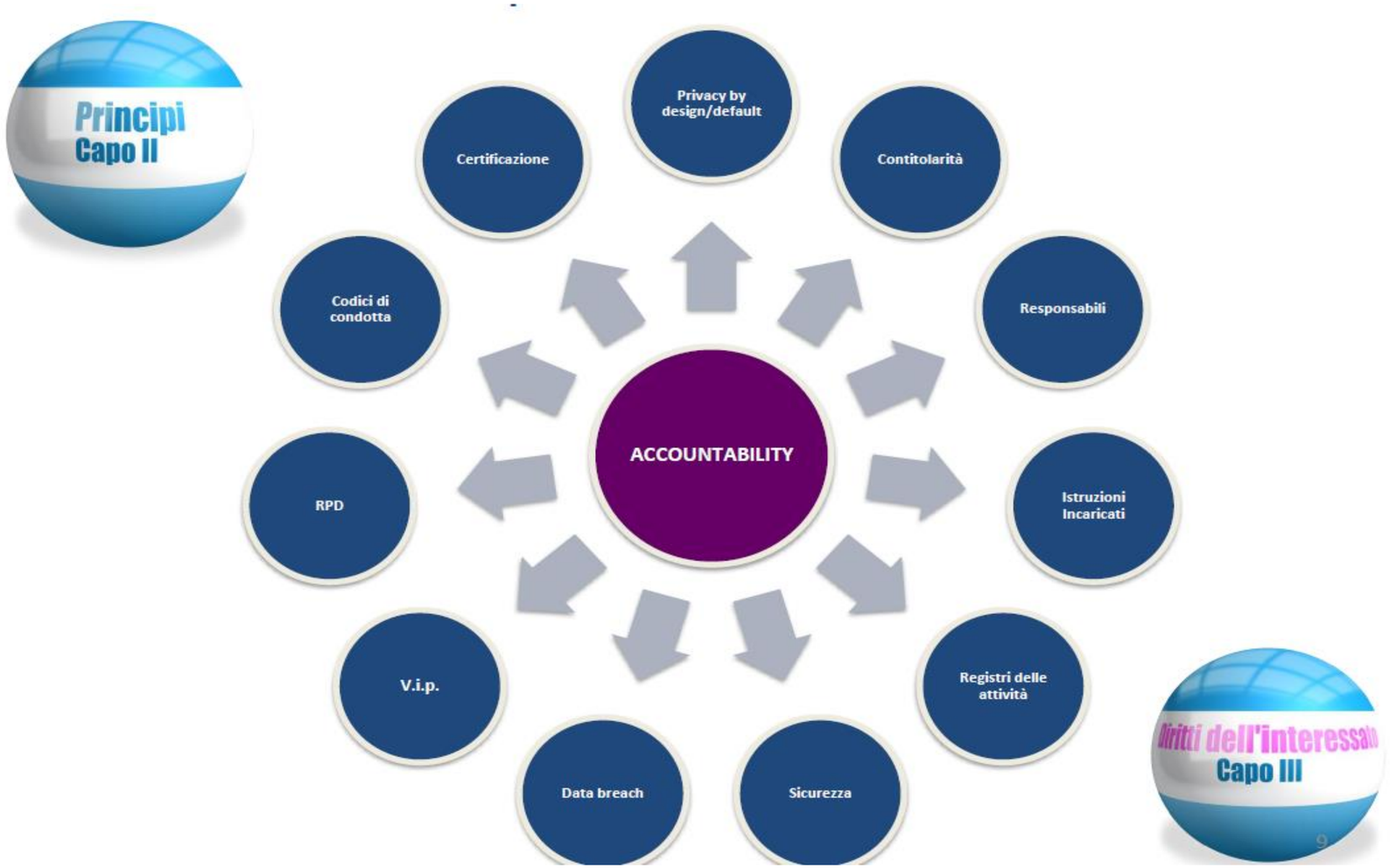
PNT CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

idea Kiwa Cermet Idea

500 giorni di GDPR

Cosa è cambiato nel mondo della protezione dei dati personali?

L'IMPORTANZA DI UN METODO



Unione Province d'Italia UPI Emilia-Romagna

PNT CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

idea Kiwa Cermet Idea

REGOLAMENTO EUROPEO 2016/679 – LA VALORIZZAZIONE DELLE CERTIFICAZIONI

- Gli Stati membri, le Autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano, **l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati**, allo **scopo di dimostrare la conformità al Regolamento delle operazioni di trattamento effettuate dal Responsabile e dall'incaricato del trattamento** *(Considerando 100).*
- Si deve tenere conto delle esigenze specifiche delle micro, piccole e medie imprese. *(art, 42 par. 1)*
- La certificazione deve essere **volontaria** e **disponibile attraverso un procedimento trasparente**.

REGOLAMENTO EUROPEO 2016/679 – LA VALORIZZAZIONE DELLE CERTIFICAZIONI (2)

- Il ricorso alle certificazioni può essere utilizzato per individuare gli orientamenti necessari per mettere in atto misure opportune e per dimostrare la compliance del titolare o del responsabile con particolare riferimento «*all'**individuazione del rischio** connesso al trattamento, la sua **valutazione** in termini di origine, natura, probabilità e gravità, e **l'individuazione** di **migliori prassi** per **attenuare il rischio**» (Considerando 77*).
- Inoltre l'**applicazione** da parte del responsabile di un **meccanismo di certificazione** può essere utilizzata da parte del titolare come **elemento per dimostrare** il rispetto degli obblighi regolamentari *(Considerando 81).*
- La **certificazione non riduce la responsabilità del Titolare o del Responsabile** del trattamento in merito ai loro compiti né pregiudica le funzioni e i poteri dell'Autorità di controllo competente.

REGOLAMENTO EUROPEO 2016/679 – LA VALORIZZAZIONE DELLE CERTIFICAZIONI (3)

- La certificazione è rilasciata dagli organismi di certificazione o dall'Autorità di controllo.
- Il Titolare o il Responsabile, che sottopone il trattamento dei dati al meccanismo di certificazione, **deve fornire** all'organismo di certificazione o all'Autorità di controllo competente, **tutte le informazioni e l'accesso alle attività di trattamento, che sono necessari per la procedura di certificazione**.
- Lo sviluppo di sistemi di certificazione dovrebbe concentrarsi sulla **verificabilità**, **significatività** ed **idoneità** dei criteri di certificazione a dimostrare la conformità con il Regolamento.

LA PRASSI DI RIFERIMENTO UNI/PDR 43:2018

A settembre 2018 è stata pubblicata da UNI la Prassi di Riferimento **UNI/PdR 43:2018** “Linee guida per la gestione dei dati personali in ambito ICT secondo il Regolamento UE 679/2016 (GDPR)”.

Questa **linea guida** è stata elaborata dal Tavolo **“Processi di gestione privacy in ambito digitale”**, sotto il coordinamento di **UNINFO**, Ente Federato all’UNI, che lavora nell’ambito delle tecnologie informatiche e delle loro applicazioni.

Ha lo **scopo** di **definire in modo obiettivo e ripetibile le azioni corrette per garantire particolari trattamenti di dati nell’ambito ICT,** in modo da offrire ai Titolari e Responsabili una guida di riferimento ed alle Autorità di controllo un metro di giudizio, ponendo le basi per i meccanismi di certificazione come auspicati dall’art. 42 e 43 del GDPR.

LA UNI/PDR 43:2018 ED IL QUADRO EUROPEO

- Il 4 giugno 2019 European Data Protection Board (Comitato europeo per la protezione dei dati) ha adottato al versione finale dell'Annex 2 "Guidelines on Certification". Lo scopo principale di queste linee guida è identificare i criteri generali che possono essere rilevanti per tutti i tipi di meccanismi di certificazione emessi in conformità con gli art. 42 and art. 43 del GDPR.
- In Italia il Garante e Accredia identificheranno gli adempimenti aggiuntivi che permetteranno di completare la «compliance» della UNI/PdR all'art. 42.
- E' uno strumento che aiuta a traghettare le aziende da una logica di privacy "a sequenza di singoli adempimenti" a logica "di Sistema di gestione virtuoso"
- E' focalizzata sui trattamento dei dati personali, mediante strumenti elettronici (ICT)

SEZIONE 1 DELLA UNI/ PDR 43:2018

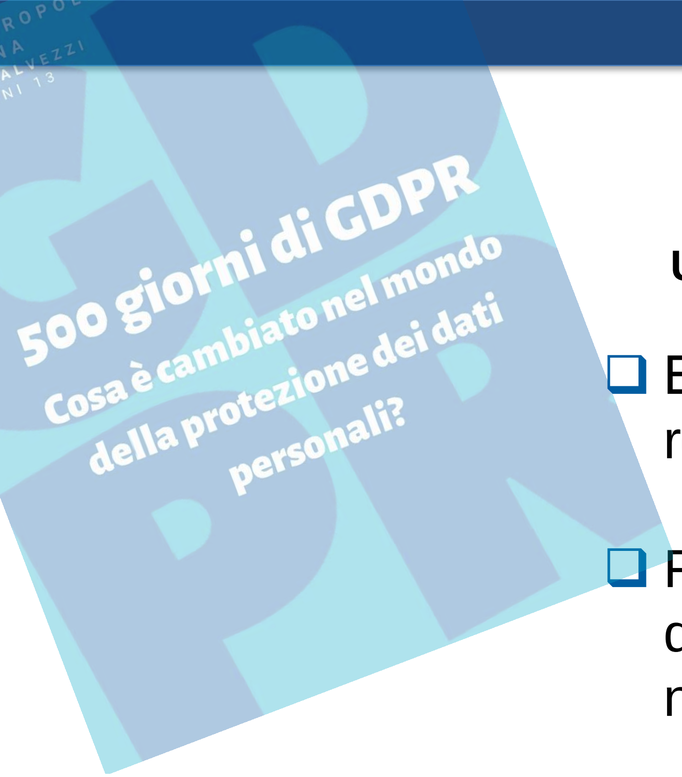
La norma è suddivisa in due sezioni:

UNI/PdR 43.1:2018 - Gestione e monitoraggio dei dati personali in ambito ICT

- Fornisce le linee guida a supporto della gestione e monitoraggio dei processi e delle attività definite nel Regolamento Europeo 2016/679 in riferimento al trattamento dei dati personali.

- Tali attività si basano su infrastrutture e processi tipici dell'ambito informatico.

- Mappa e definisce i principali processi al fine di permettere alle organizzazioni la corretta implementazione, il conseguente controllo e l'eventuale certificazione del servizio a tutela del mercato.



SEZIONE 2 DELLA UNI/ PDR 43:2018

UNI/PdR 43.2:2018 – Requisiti per la protezione e valutazione di conformità dei dati personali in ambito ICT

- E’ applicabile a tutte le organizzazioni che, in qualità di titolari e/o responsabili del trattamento, gestiscono dati personali con strumenti ICT.
- Finalizzata a fornire un insieme di requisiti che permetta a questi soggetti di essere conformi a quanto previsto dal quadro normativo europeo e nazionale in modo efficace.
- Fornisce inoltre gli indirizzi per la valutazione di conformità ai requisiti definiti.
- **La sezione 2 è certificabile.**

Unione Province d'Italia UPI Emilia-Romagna
CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

DESTINATARI DELLA PRASSI

Società (persone giuridiche e/o persone fisiche) che trattano dati personali mediante strumenti elettronici (ICT).

La certificazione alla prassi può essere richiesta da qualunque organizzazione, di qualsiasi dimensione e/o settore lavorativo, indipendentemente dalla sua forma giuridica.

Permette alle organizzazioni, in particolare alle PMI, di essere conformi a quanto previsto dal quadro normativo europeo e nazionale in modo efficace, potendo dimostrare tale conformità ed efficacia anche attraverso un percorso di certificazione.

500 giorni di GDPR

Cosa è cambiato nel mondo della protezione dei dati personali?

LA STRUTTURA DELLA UNI/PDR 43.2:2018

Suddivisione in 3 CAPITOLI che si rifanno al classico ciclo PDCA

PIANIFICAZIONE

ATTIVITA' OPERATIVE

CONTROLLO (e correzione)

Unione Province d'Italia
UPI
Emilia-Romagna

PNT
CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

idea
Kiwa Cermet Idea

LA STRUTTURA DELLA UNI/PDR 43.2:2018 – PIANIFICAZIONE

CAPITOLO DELLA NORMA	RIFERIMENTI NORMATIVI
5.1 COMPRENDERE L'ORGANIZZAZIONE E IL SUO CONTESTO	•Art. 24 GDPR «Responsabilità Del Titolare»
	•Art. 26 GDPR «Contitolari»
	•Art. 27 GDPR «Rappresentanti di titolari del trattamento o dei responsabili del trattamento»
	•Art. 28 GDPR «Responsabile del trattamento»
	•Artt.37-39 «DPO»
	•Art. 4 punto 10 «Persone autorizzate al trattamento»
	•Art. 2 quaterdecies d.lgs.196/203 novellato dal d.lgs.101/2018 «Attribuzione di funzioni e compiti a soggetti designati»
	•Provv. Garante 27/11/2008 e s.m.i. «Amministratori di sistema»
5.2 AMBITO DELLA PROTEZIONE DEI DATI PERSONALI	
•5.2.1 INVENTARIO E FLUSSO DEI DATI (REGISTRO)	• Art. 30 GDPR "Registro delle attività di trattamento"
•5.2.2 INDIVIDUAZIONE DELLE BASI LEGALI	• Art. 6 GDPR "Liceità del trattamento" Art. 2-sexies d.lgs.196/203 novellato dal d.lgs.101/2018 (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante)
5.3 POLITICA PER LA PROTEZIONE DEI DATI PERSONALI	•Art. 5 GDPR "Principi applicabili al trattamento di dati personali"
5.4 RUOLI E RESPONSABILITÀ	
•5.4.1 POSIZIONI INTERNE	•Approfondimento di 5.1 COMPRENDERE L'ORGANIZZAZIONE E IL SUO CONTESTO
	Profili previsti dalla UNI 11697:2017
•5.4.2 POSIZIONI ESTERNE	•Approfondimento di 5.1 COMPRENDERE L'ORGANIZZAZIONE E IL SUO CONTESTO
	Profili previsti dalla UNI 11697:2017
5.5 GESTIONE DEL RISCHIO	
•5.5.1 VALUTAZIONE DEL RISCHIO E D'IMPATTO SULLA PROTE	•Art. 35 GDPR "Valutazione d'impatto sulla protezione dei dati"
•5.5.2 TRATTAMENTO DEL RISCHIO E PIANO DI TRATTAMENT(	•Art. 32 "Sicurezza del trattamento"
•5.5.3 PROTEZIONE DEI DATI PERSONALI BY DESIGN E BY DEF/	•Art. 25 GDPR "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"
5.6 PIANIFICAZIONE DELLE MODIFICHE	•Art. 5.2 "Accountability del titolare"

Unione Province d'Italia UPI Emilia-Romagna

PNT CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE

idea Kiwa Cermet Idea

LA STRUTTURA DELLA UNI/PDR 43.2:2018 – ATTIVITA' OPERATIVE

CAPITOLO DELLA NORMA	RIFERIMENTI NORMATIVI
6.1 INFORMATIVE E CONSENSI	
•6.1.1 INFORMATIVE	•Artt. 13 e 14 del GDPR "Informative di dati raccolti e NON raccolti presso l'interessato"
•6.1.2 CONSENSI	•Art. 6.1.a GDPR "Consenso«
6.2 AGGIORNAMENTO DELLE POSIZIONI	•Art. 5.2 "Accountability del titolare"
6.3 PROTEZIONE DEI DATI PERSONALI	
•6.3.1 MINIMIZZAZIONE DEI DATI	•Art. 25 GDPR "Protezione dei dati fin dalla progettazione e protezione per impostazion predefinita"
•6.3.2 CONSERVAZIONE E CANCELLAZIONE DEI DATI	•Art. 5.1.e e art. 13.2.a "Periodi e criteri di conservazione de i dati"
•6.3.3 ATTUAZIONE E MANTENIMENTO DELLE MISURE DI SICU	•Art. 32.1.d "verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento"
• 6.3.4 GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI	•Artt. 33 e 34 "Violazioni di dati personali"
6.4 RICHIESTE DI ESERCIZIO DEI DIRITTI DEGLI INTERESSATI	•Artt. 15-22 del GDPR "Diritti degli interessati"
•6.4.1 ACCESSO AI DATI	
•6.4.2 RETTIFICA	
•6.4.3 ELIMINAZIONE	
•6.4.4 LIMITAZIONE DI TRATTAMENTO	
•6.4.5 PORTABILITÀ DEI DATI	
•6.4.6 OPPOSIZIONE	
•6.4.7 DECISIONI AUTOMATIZZATE, COMPRESA LA PROFILAZIONE	
•6.4.8 RECLAMI E RICORSI	
6.5 FORMAZIONE E CONSAPEVOLEZZA	•Art. 28.3.a "tratti i dati personali soltanto su istruzione documentata del titolare del trattamento"

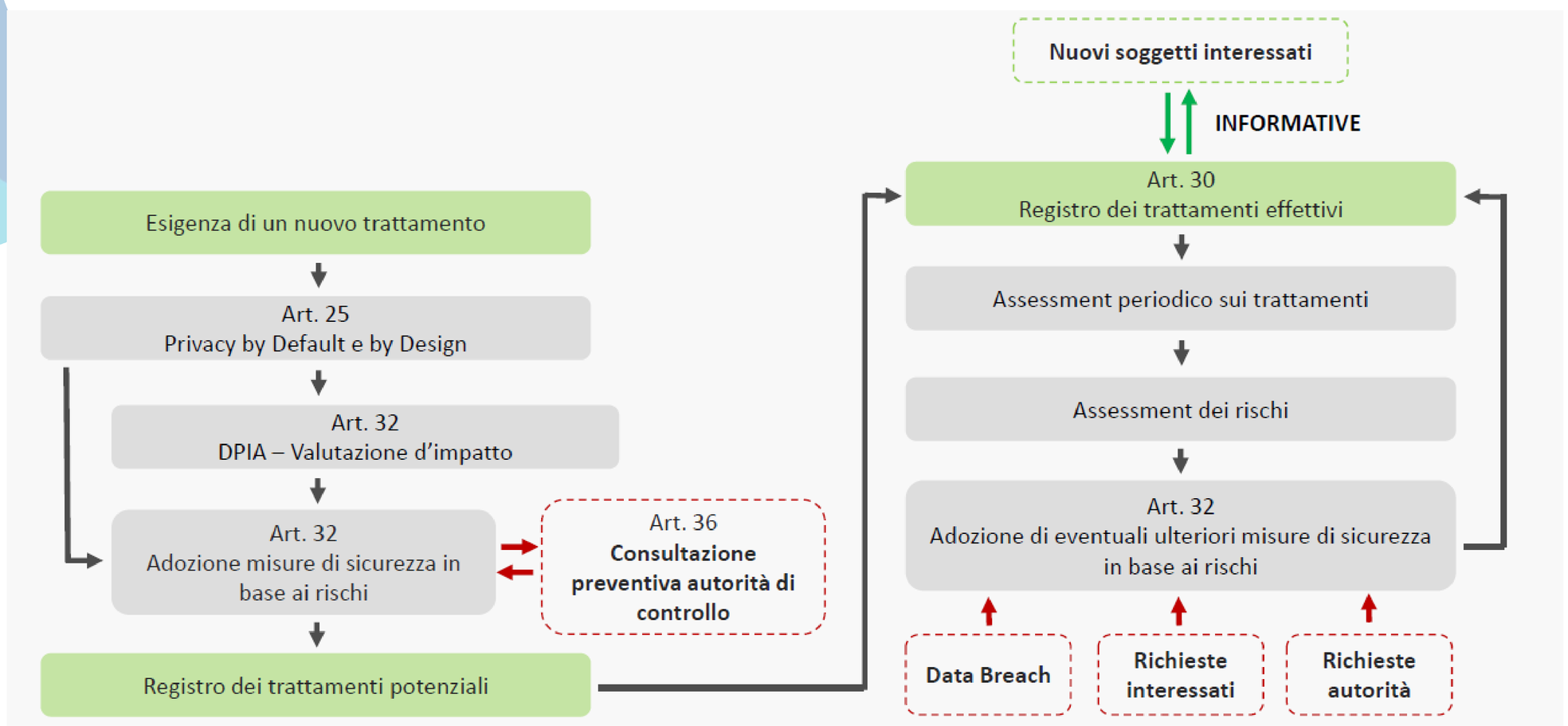
Unione Province d'Italia UPI Emilia-Romagna
CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

LA STRUTTURA DELLA UNI/PDR 43.2:2018 – CONTROLLO

CAPITOLO DELLA NORMA	RIFERIMENTI NORMATIVI
7.1 AUDIT INTERNO	•Art. 5.2 "Accountability del titolare"
7.2 RELAZIONE PERIODICA	•Art. 5.2 "Accountability del titolare"
7.3 NON CONFORMITÀ E AZIONI CORRETTIVE	•Art.24.1.e "Responsabilità del Titolare… Dette misure sono riesaminate e aggiornate qualora necessario."

500 giorni di GDPR
Cosa è cambiato nel mondo della protezione dei dati personali?

UNI/PDR 43.2:2018 – LA PRIVACY COME SISTEMA DI GESTIONE



Unione Province d'Italia UPI Emilia-Romagna
PNT CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

L'ITER DI CERTIFICAZIONE

La norma di riferimento per la gestione dello schema di certificazione e per l'accreditamento è la norma ISO 17065, cioè la norma relativa alle certificazioni di prodotto/servizio.

Si applicano tuttavia alcuni requisiti riconducibili alla norma ISO 17021-1 relativamente alla frequenza degli audit che compongono il ciclo di certificazione e al calcolo della durata degli audit.

L'iter di certificazione segue l'iter standard di una certificazione di prodotto/servizio:

1° anno -Verifica iniziale (Analisi documentale +Stadio 2 in campo)
2° e 3° anno – Verifiche di sorveglianza
4° anno – Verifica di rinnovo

COMPETENZE DEL GRUPPO DI AUDIT

Nel gruppo di verifica i requisiti di competenza si ritengono soddisfatti quando, tenendo conto delle competenze complessive del gruppo di verifica (auditor ed eventuali Esperti Tecnici) siano presenti auditor certificati sotto accreditamento (ISO/IEC 17024) ai sensi della norma UNI 11697 (Attività professionali non regolamentate - Profili professionali relativi al trattamento e alla protezione dei dati personali - Requisiti di conoscenza, abilità e competenza).

In assenza di questa certificazione, deve essere dimostrata:

- Competenza, maturata a seguito di esperienze lavorative di almeno 8 anni, in materie attinenti la sicurezza delle informazioni e la protezione dei dati personali;
- Competenza, maturata a seguito di esperienze lavorative di almeno 8 anni, in ambito giuridico (Es: avvocato, magistrato, giurista) con comprovata esperienza nella data protection.
- Qualifica di auditor in un qualunque schema di certificazione in quanto tutti i membri del team devono conoscere ed avere familiarità con le tecniche di audit (ISO 19011).
- Conoscenza della Prassi di riferimento.

Ogni membro del team di verifica può operare in autonomia, o con la collaborazione di un esperto tecnico, in modo che complessivamente nel gruppo siano garantite le competenze esposte.

VANTAGGI E BENEFICI DELLA CERTIFICAZIONE SECONDO LA UNI/PDR 43.2:2018

- Aiuta a traghettare le aziende da una logica di privacy “a sequenza di singoli adempimenti” a logica “di Sistema di gestione virtuoso”.
- E’ uno strumento per raccogliere, diffondere e mantenere aggiornati i buoni comportamenti, permettendone la riconoscibilità, la valutazione e la condivisione.

- Per i titolari: guida di indirizzo per gestire i dati nel rispetto del regolamento (vantaggio competitivo).
- Per i responsabili: sistema di misurazione delle performance e responsabilità nel rapporto con i titolari.
- Per le Autorità di controllo: strumento di valutazione della diligenza di titolari e responsabili.
- Per gli interessati: garanzia del rispetto dei propri diritti.

Unione Province d'Italia UPI Emilia-Romagna
CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

CONVENZIONE GARANTE – ACCREDIA

- Il 27 marzo 2019 firmata la convenzione tra Garante privacy e Accredia in merito al *Regolamento Ue e certificazione accreditata in materia dei dati personali.*
- Nell'ambito della collaborazione tra il Garante per la protezione dei dati personali e Accredia, l'Ente nazionale di accreditamento, in rapporto alle attività di accreditamento e certificazione previste dal Regolamento (artt. 42 e 43), è stata sottoscritta la convenzione volta a favorire lo scambio di informazioni in merito a tali attività, nonché a valorizzare le reciproche competenze.
- Il Regolamento Ue prevede e incoraggia l'istituzione di meccanismi per la certificazione della protezione dei dati personali, nonché di sigilli e marchi, allo scopo di dimostrare la conformità dei trattamenti effettuati dai Titolari e dai Responsabili del trattamento.

CONVENZIONE GARANTE – ACCREDIA (2)

- Accredia avrà il compito di attestare - in base alla norma di accreditamento UNI CEI EN ISO/IEC 17065:2012, integrata da “requisiti aggiuntivi” che saranno individuati dal Garante sulla base delle linee-guida comuni elaborate in seno al Comitato europeo per la protezione dei dati - la competenza e l’adeguatezza degli Organismi che ne faranno richiesta per certificare con maggiori garanzie i servizi di tutela della privacy.
- In base all’accordo, Accredia comunicherà all’Autorità gli accreditamenti rilasciati, i ricorsi degli Organismi accreditati e le decisioni assunte, le scadenze dei certificati, i provvedimenti sanzionatori, l’elenco delle certificazioni e le relative revoche e sospensioni rilasciate dagli Organismi. Il Garante comunicherà ad Accredia gli aggiornamenti della normativa, le novità sugli schemi di certificazione approvati a livello nazionale ed europeo, nonché le informazioni su problematiche che potrebbero emergere da reclami pervenuti all’Autorità.
- La Convenzione ha la durata di un anno con tacito rinnovo per un ulteriore anno.

STRUMENTI ULTERIORI A SUPPORTO DELLE ORGANIZZAZIONI

- **ISO 27001 e linee guida correlate**, tra cui:
  - ISO 27017 e ISO 27018 riguardanti i fornitori di servizi cloud, obbligatori per lavorare con il settore pubblico.
  - ISO 27701 estensione dei controlli privacy della ISO 27001.
- **Vulnerability assessment/ penetration tests** per le aziende che intendano verificare la solidità del proprio sistema informativo (per questi servizi Accredia ha richiesto alle aziende che erogano servizi di conservazione sostitutiva o eIDAS entro un anno di utilizzare laboratori accreditati da Accredia secondo la ISO / IEC 17025: 2005).
- **Certificazione figura professionale DPO (e le altre figure professionali in ambito privacy)** secondo la UNI 11697

2020 - UNA NUOVA FASE DEL GDPR

- I dati personali oggi sono il business o, più precisamente, sono la materia prima del business: sono le persone fisiche che votano, lavorano, comprano prodotti e servizi e ne fruiscono, direttamente o indirettamente.

- Il GDPR contrasta il far west nell'uso di dati personali, che ha caratterizzato la fase nascente della digital economy e disegna un nuovo contesto in cui le aziende e organizzazioni pubbliche e sociali avranno bisogno di comunicare e realizzare prodotti e servizi in modo più mirato e personalizzato, utilizzando l'innovazione digitale.

2020 - UNA NUOVA FASE DEL GDPR (2)

Se ad oggi i progetti erano di adeguamento (registro trattamenti, informative e consensi), la nuova fase del GDPR dovrà prendere in considerazione altri aspetti:

- **Processo di innovazione**: Articoli 25 (Protezione dati fin dalla progettazione), 35 (valutazione d'impatto sulla protezione dei dati) e 36 (consultazione preventiva)

- **Presidio e gestione della sicurezza dei dati personali: Articoli** 32 (Sicurezza del trattamento), 33 (Notifica di una violazione all'Autorità di controllo)

- **Gestione delle responsabilità e catena di fornitura:** Articolo 28 (Responsabile del trattamento)

Unione Province d'Italia UPI Emilia-Romagna
CENTRO STUDI PRIVACY E NUOVE TECNOLOGIE
idea Kiwa Cermet Idea

GRAZIE DELL'ATTENZIONE!

Unione Province d'Italia
UPI
Emilia-Romagna

PNT
CENTRO STUDI
PRIVACY E NUOVE
TECNOLOGIE

idea
Kiwa Cermet Idea