Report annuale del DPO e pianificazione

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy.
Membro del Comitato Scientifico del CLUSIT.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Oltre 150 corsi e seminari presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CEFRIEL, ABI…
Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei.
Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate.
Ha pubblicato 26 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 27 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di AIEA è socio del CLUSIT e del BCI.
Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.blog.europrivacy.info .
Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.

Note sul copyright

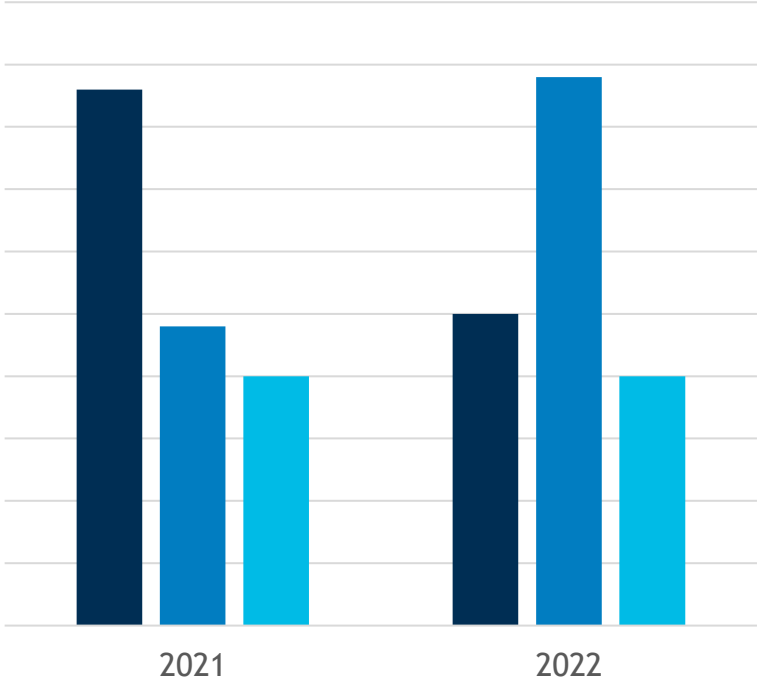
Alcuni testi derivano da queste mie pubblicazioni

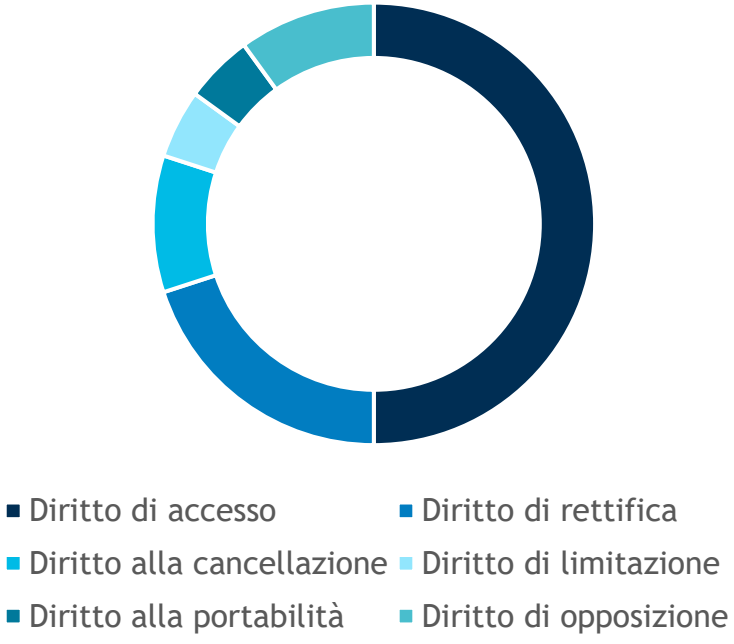
Note sul copyright

- Le verifiche in ambito privacy
- Caratteristiche degli audit in ambito privacy
- Realizzare un assessment iniziale
- Audit in pratica
- La verifica dei vari requisiti normativi
- Audit dei sistemi informativi
- Audit delle misure di sicurezza
- L'audit degli aspetti normativi

Attività di consulenza
Data breach
Esercizio dei diritti
Pareri sulle DPIA
Formazione
Interazione con l'autorità di controllo

Relazione annuale - Attività ex ante – Data breach




Diritto di accesso
Diritto di rettifica
Diritto alla cancellazione
Diritto di limitazione
Diritto alla portabilità
Diritto di opposizione

Attività di audit sul modello privacy del Titolare
Verifiche in merito alla aderenza dei comportamenti al modello privacy del titolare

TIPOLOGIA DI AUDIT in ambito privacy

- Audit ambiti formalizzati
- Audit ambiti non formalizzati

- Audit verticali su singole tematiche
- Audit orizzontali di processo

- Assesment complessivi
- Valutazione di adeguamento

TIPOLOGIA DI AUDIT in ambito privacy

- Audit su ambiti formali:
  - Informative
  - Designazioni
  - Basi giuridiche
- Audit su ambiti non formalizzati
  - Misure di sicurezza
  - Analisi dei rischi
- Audit su temi specifici:
  - Amministratori di Sistema
  - Videosorveglianza
  - Firma grafometrica
  - …
- Audit tecnici/organizzativi specifici:
  - Profilazione degli utenti
  - Tempi di conservazione
  - Esercizio dei diritti
  - Qualità dei dati
  - …

SINTESI DEI RISULTATI

L'attività di audit ha riguardato:

- la verifica delle policy e procedure relative alla:
  - gestione delle strutture organizzative (nuovi uffici, accorpamenti, eliminazione…)
  - definizione di mansionari per le strutture con un livello di dettaglio sufficiente a individuare attività, strumenti, documenti, dati, flussi in ingresso e flussi in uscita
  - definizione dei ruoli
  - definizione dei profili autorizzativi
  - abbinamento ruoli/profili
  - gestione degli utenti (censimento iniziale, variazione di ruolo, assenze prolungate, cessazione del rapporto…)
- la gestione degli utenti ed il loro censimento sul sistema informativo
- l'implementazione e gestione dei profili sul sistema informativo.

L'attività di audit ha ricompreso la verifica degli aspetti formali, operativi ed i relativi controlli.

L' audit ha rilevato:

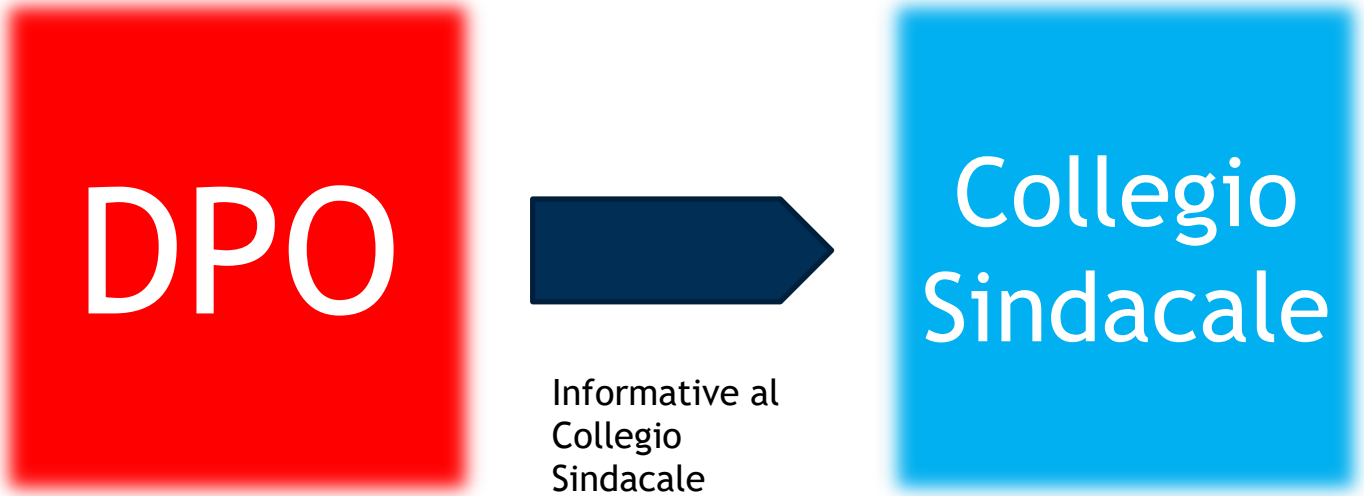
- le procedure in essere non consentono una mappatura sufficientemente dettagliata delle attività svolte dai singoli uffici

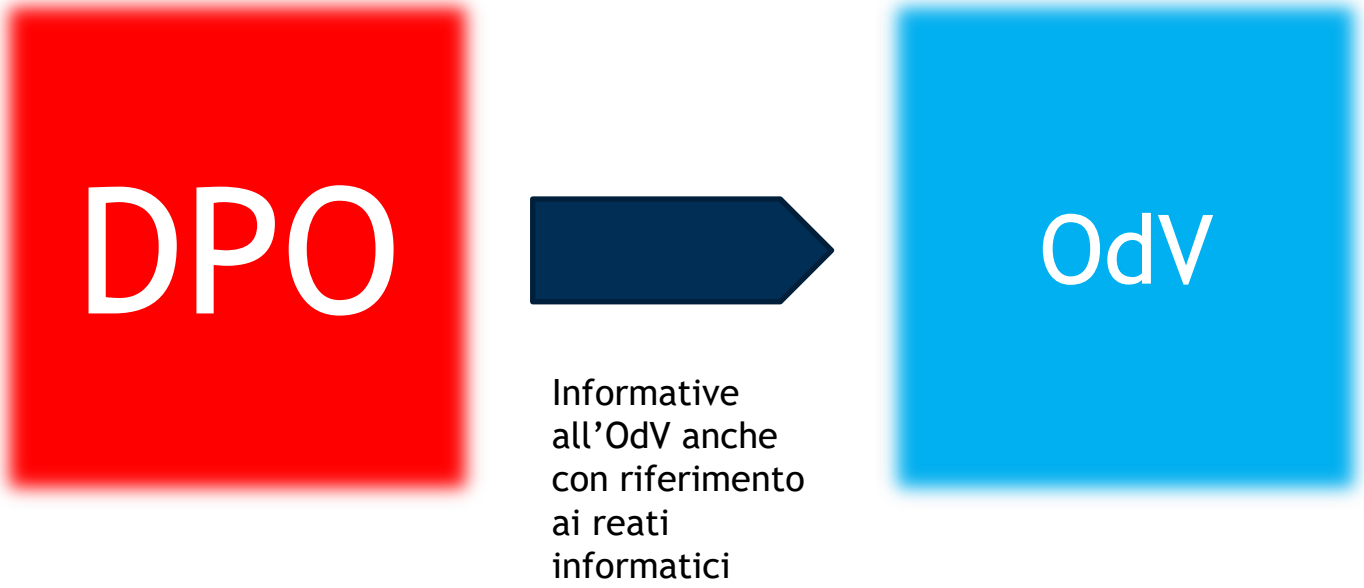
- manca una specifica procedura in merito all'attribuzione delle autorizzazioni ad personam
- la definizione dei profili abilitativi viene effettuata senza un reale censimento delle singole funzioni disponibili sulle applicazioni
- il censimento dei profili abilitativi sul catalogo dei profili viene effettuato senza regole condivise
- la descrizione dei profili abilitativi nel catalogo non consente di capire nel dettaglio quali siano le reali autorizzazioni abbinate al singolo profilo
- non risultano censite le abilitazioni ad personam
- non vi è una corrispondenza univoca fra i ruoli definiti nella procedura del personale e quelli nelle procedure che gestiscono la sicurezza.

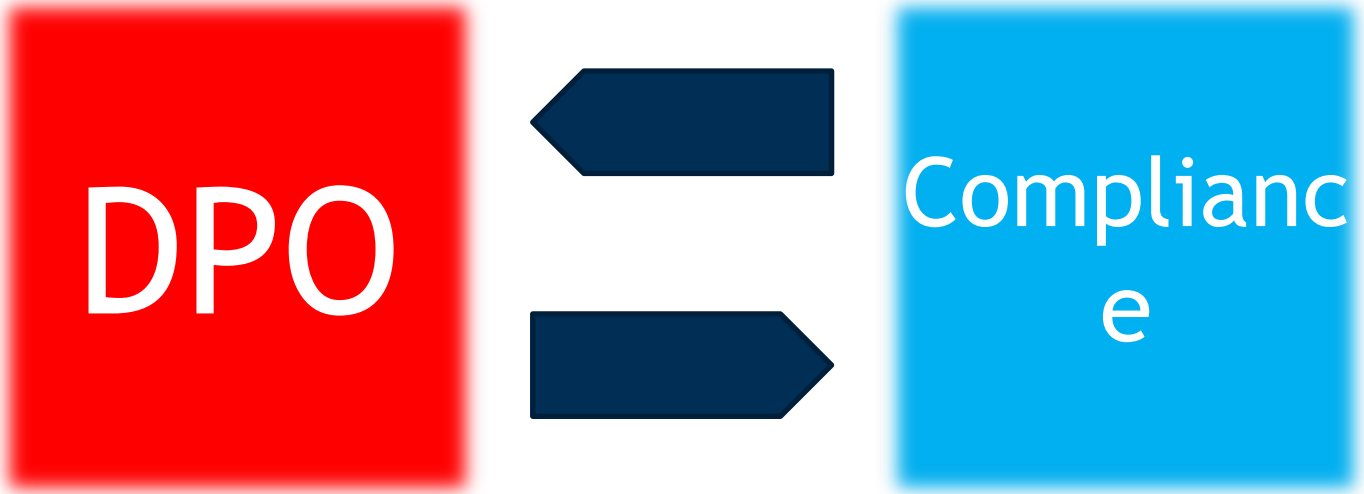
Sono stati inoltre riscontrati dall'analisi di 100 utenti (10% del totale):

- 3 utenti con l'attribuzione di un ruolo sul sistema informativo del personale non corrispondente all'ufficio di appartenenza
- 1 utente ancora censito come operativo anche se risulta essere dimissionario da 15 giorni precedente l'attività di verifica
- 2 utenti con autorizzazione ad personam non in linea con il loro attuale ruolo, ma compatibili con il precedente ruolo
- 1 utente con attribuzione di un profilo autorizzativo non in linea con il ruolo.

Collegio sindacale

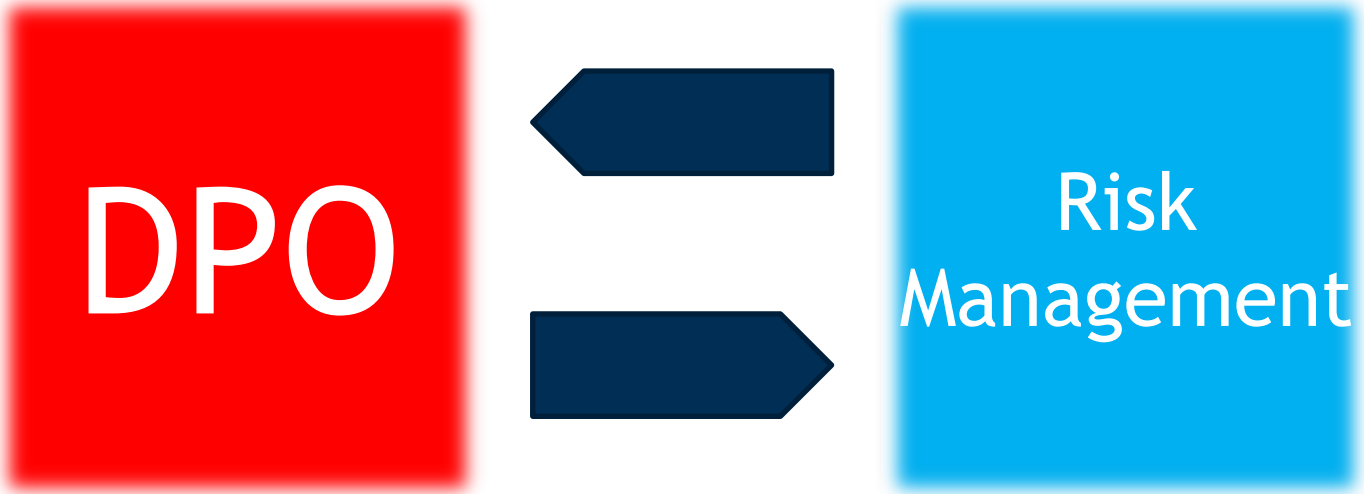



DPO
OdV
Informative all'OdV anche con riferimento ai reati informatici

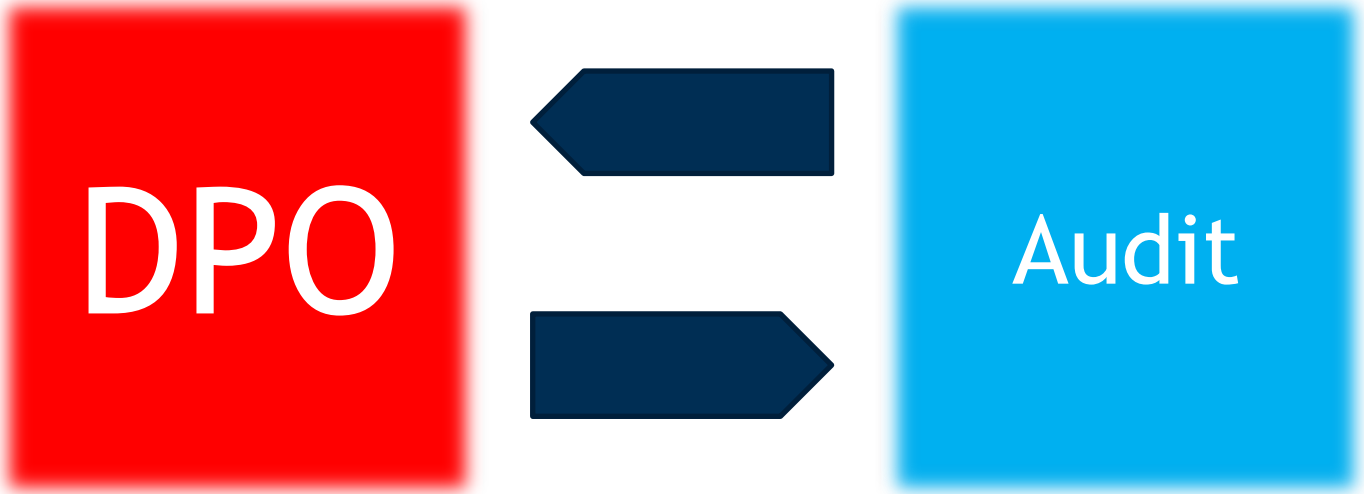


Scambio di informazioni sui rispettivi controlli in ambito privacy

Risk management function

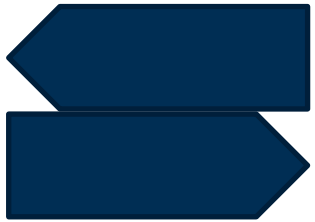


Scambio di informazioni sulla valutazione dei rischi e sulla PIA



Scambio di informazioni sui rispettivi controlli in ambito privacy

DPO



Legale

- Opinioni
- Contratti In Essere
- Nuovi Contratti
- Nuovi Progetti


DPO
IT
• ICS, KPI
• Nuovi Progetti
• Variazioni al Sistema Informativo

DPO

Sicurezza IT

- Controlli
- Implementazioni di sicurezza
- Variazioni alle misure di sicurezza
- Incidenti di sicurezza

DPO

- Variazioni di personale
- Variazione di ruoli
- Assessment

HR

DPO

- Nuovi Progetti
- Variazioni organizzative
- Nuovi Progetti

Organizzazione

Driver per la selezione delle aree da sottoporre a verifica:

- Aree dove maggiore è il rischio per i diritti e le libertà delle persone fisiche
- Aree individuate dell'Autorità Garante nel suo piano di ispezioni
- Aree dove maggiore è il rischio per l'organizzazione
- Aree non coperte da precedenti verifiche

- liceità del trattamento
- condizioni per il consenso
- consenso dei minori in relazione ai servizi della società dell'informazione
- trattamento di categorie particolari di dati
- trattamenti relativi a condanne e reati
- trattamenti che non richiedono identificazione
- diritti degli interessati: trasparenza delle informazioni
- diritti degli interessati: informazioni da fornire se i dati sono ottenuti dagli interessati
- diritti degli interessati: informazioni da fornire quando i dati sono ottenuti da terzi
- diritti degli interessati: diritto di accesso
- diritti degli interessati: diritto di rettifica
- diritti degli interessati: diritto alla canceallazione ("il diritto all'oblio")
- diritti degli interessati: diritto alla limitazione del trattamento
- diritti degli interessati: rettifica, cancellazione, limitazione del trattamento
- diritti degli interessati: diritto alla portabilità dei dati
- diritti degli interessati: diritto alla portabilità dei dati
- diritti degli interessati: diritto di opposizione
- diritti degli interessati: decisioni automatizzate, inclusa la profilazione
- responsabilità del Titolare del trattamento
- privacy by design e by default
- contitolare del trattamento
- responsabile del trattamento
- registrazione delle attività di trattamento
- sicurezza del trattamento
- notifica di violazioni dei dati personali all'autorità di controllo
- comunicazione di una violazione agli interessati
- valutazione d’impatto sulla protezione dei dati
- DPO
- trasferimenti verso paesi terzi o organizzazioni internazionali.

PRINCIPIOS RELATIVOS AL TRATAMIENTO	
Se recogen los datos personales con fines determinados	
Se recogen los datos personales con fines explícitos	
Se recogen los datos personales con fines legítimos	
Se tratan ulteriormente de manera incompatible con otros fines	
Los datos personales se mantienen exactos	
Se mantienen actualizados	
Se rectifican los datos personales inexactos respecto de la finalidad	
Se suprimen los datos personales inexactos respecto de la finalidad	
Se mantienen durante más tiempo del necesario respecto de la finalidad	
Se tratan con fines de archivo en interés público	
Se tratan con fines de investigación científica	
Se tratan con fines históricos	
Los datos personales se tratan con fines estadísticos	
Se han implantado medidas de seguridad para proteger la integridad y confidencialidad de los datos	
Se han implantado medidas de seguridad contra el tratamiento no autorizado o ilícito de los datos	
Se han implantado medidas de seguridad para evitar su pérdida, destrucción o daño accidental	
Se mantiene la trazabilidad de los fines del tratamiento	

Grazie per l’attenzione

giancarlo.butti@promo.it

338 9230742