Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

Professione Dpo, una "cassetta degli attrezzi" per gestire tutte le attività

LINK: https://www.agendadigitale.eu/sicurezza/privacy/professione-dpo-una-cassetta-degli-attrezzi-per-gestire-tutte-le-attivita/

Professione Dpo, una "cassetta degli attrezzi" per gestire tutte le attività Home Sicurezza digitale Privacy Condividi questo articolo A un anno dall'entrata in vigore del Gdpr il ruolo del Data Protection Officer rimane ancora poco definito. Ma la predisposizione di un sistema di verifiche programmate può rivelarsi un ottimo strumento di lavoro. Ecco una serie di consigli pratici 11 minuti fa Giuseppe Vaciago Partner R&P Legal e fondatore di Tech&Law Center Stiamo entrando nel secondo anno di vita del GDPR e ancora il ruolo del Responsabile per la Protezione dei dati (RPD o DPO) non ha assunto contorni chiari e definiti nel contesto nazionale. L'unica certezza è che ogni DPO si sarà sentito almeno una volta come un pioniere alla ricerca di terre inesplorate (la inquietante 'Data Retention Island' o il meraviglioso, quanto pericoloso e strumentalizzato 'Portability Lake') nel disperato tentativo di dare un senso all'indecifrabile enigma dell'accountability. I dati formalizzatidall'Autorità Garante per la Protezione dei Dati Personali ci dicono che sono stati designati 48.591 Data Protection Officer nel periodo maggio 2018-marzo 2019. Sono numeri importanti che attestano una certa sensibilità da parte dei titolari dei trattamenti a investire sul nuovo Regolamento Europeo. Tuttavia, va ammesso, senza con ciò cadere in superficiali generalizzazioni, che in alcuni casi si è avuta la sensazione che la nomina del DPO fosse percepita dal titolare del trattamento come una panacea in grado di porre fine a tutte i 'mali' del GDPR confondendo questa figura con quella del consulente privacy. Il DPO, ai sensi dell'art. 39 del GDPR, dovrebbe svolgere i seguenti compiti: (i) informare e fornire consulenza in materia di protezione dei dati personali; (ii) sorvegliare l'osservanza del GDPR; (iii) fornire, se richiesto, un parere in merito alla DPIA; (iv) cooperare con l'autorità di controllo e (v) fungere da punto di contatto per quest'ultima. Ho usato il condizionaleperché nella realtà, il DPO, sia nel mondo pubblico che in quello privato, ha fornito perlopiù consulenza, rischiando di cadere talvolta nella 'tentazione' di redigere documenti e modelli che in realtà avrebbe avuto il compito di verificare. Indice degli argomenti Tutti i compiti del Dpo: il "kit" per facilitare il lavoro Ecco come pianificare le otto principali attività Tutti i compiti del Dpo: il "kit" per facilitare il lavoro Il paradigma del 'controllore' che 'controlla se stesso' è un rischio che si può verificare soprattutto nelle realtà (piccole o grandi che siano) in cui la privacy viene - purtroppo - ancora percepita come un costo e non come una opportunità. Una soluzione potrebbe essere quella di predisporre un ferreo piano di attività basato su un sistema di verifiche programmate in grado di mettere nelle condizioni il titolare del trattamento di effettuare, con l'ausilio del DPO, una serie di controlli periodici in ambito GDPR. Insieme ad un gruppo di DPO di comprovataesperienza, ho dato il mio contributo per realizzare un software in grado di gestire tale piano di attività che consente di guidare il DPO nel monitoraggio periodico delle varie aree di criticità di applicazione del GDPR. Questa esperienza è stata utile per comprendere il bisogno di ciascun DPO di razionalizzare la propria attività di verifica rendendola un processo organizzato e per quanto possibile automatizzato. Non vorrei però essere frainteso: non credo (o, meglio, non credo ancora) nella gestione della privacy attraverso un algoritmo intelligente in grado di sostituirsi alle competenze giuridiche e tecnologiche del professionista che, per anni, ha studiato questa materia. Tuttavia, ritengo che, per poter 'sopravvivere' soprattutto in questa prima fase applicativa, sia necessario uno strumento che sia di ausilio al titolare del trattamento dei dati e al DPO da questi designato. Lo strumento non deve essere

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

necessariamente un software (può essere anche un foglio excel), ma èsicuramente utile (se non essenziale) allo scopo. Fatte queste premesse, vi riporto di seguito alcune aree di attività dove è necessario intervenire con verifiche puntuali attraverso delle check-list realizzate ad hoc da chi ha acquisito una valida esperienza sul campo. Ecco come pianificare le otto principali attività Verifica del registro delle attività di trattamento del Titolare o del responsabile. L'obbligo di tenuta di tale registro incombe sul Titolare o sul responsabile, ma come ricordano le Linee Guida WP29 (ora EPBD) sul ruolo del DPO (punto 4.5), l'art. 39 co. 1 contiene un elenco minimo dei compiti affidati al DPO. L'obbligo di sorveglianza finalizzato all'aggiornamento di tali registri è sicuramente un'attività che può e deve essere svolta da quest'ultimo, in quanto consente di avere un quadro di insieme dei trattamenti compiuti dal Titolare e di valutare l'opportunità di effettuare delle valutazioni di impatto nel caso essi comportino un rischio elevato per i diritti ele libertà degli interessati. Verifica del contenuto delle informative. A partire dal registro delle attività di trattamento, tenuto a cura del Titolare o del responsabile, il DPO deve verificare il contenuto delle informative raccolte presso l'interessato o presso terzi, la tempistica e le modalità della comunicazione ed eventuali modifiche intervenute nel tempo. Liceità del trattamento. L'art. 5 del GDPR prescrive che i dati personali debbano essere trattati 'in modo lecito, corretto e trasparente nei confronti dell'interessato'. L'articolo 6 del GDPR elenca le basi giuridiche del trattamento che, come noto, sono: (i) consenso; (ii) esecuzione di un contratto; (iii) obbligo legale; (iv) salvaguardia degli interessi vitali; (v) interesse pubblico; (vi) interesse legittimo. Una verifica puntuale in tal senso è fondamentale, soprattutto in tema di gestione del consenso. Trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali. Il DPO deve verificare eventualitrasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali al fine di aggiornare il registro delle attività di trattamento o le informative ove, ad esempio, fosse sfuggita una piattaforma in cloud che conserva alcuni dati personali degli interessati per conto del Titolare. Attività di formazione del personale. Tra i compiti specifici del DPO, l'art. 39 co. 1 lett. b) del GDPR menziona '... la sensibilizzazione e la formazione del personale che partecipa ai trattamenti'. Il DPO deve, quindi, predisporre un piano di formazione che possa consentire a coloro che trattano i dati di acquisire un buon grado di consapevolezza della normativa in generale e delle procedure in particolare (ad es. in materia di data breach). La creazione di un sistema in grado di documentare tutte le iniziative di formazione è fondamentale in caso di verifica dell'Autorità (dal registro delle presenze durante le giornate di formazione alla creazione di report che certificano l'attività die-learning e i relativi test di verifica). L'analisi del rischio e in particolare il controllo della sussistenza dei requisiti essenziali di sicurezza informatica. Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate a garantire la sicurezza dei dati personali, così come richiesto dagli articoli 25 e 32. Per raggiungere tale scopo ha il compito di monitorare costantemente la sussistenza di alcuni requisiti essenziali in tema di gestione della sicurezza delle informazioni. In questo caso, la check-list di controllo costituisce un valido strumento per poter perimetrare l'ambito e il grado di urgenza di un più approfondito audit IT. La verifica dei requisiti del responsabile esterno del trattamento. La verifica di idoneità del responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR non è un'attività che dovrebbe svolgere il DPO in prima persona per le ragioni dette in premessa, ma quest'ultimo deve assistere il titolare nella creazione diuna metodologia di controllo efficace e coerente con le attività svolte dai singoli responsabili esterni. Inoltre, il DPO deve creare un sistema che consenta il costante monitoraggio della corretta contrattualizzazione con i responsabili esterni. L'attribuzione delle responsabilità

Agenda Digitale.eu
IL PRIMO GIORNALE SULL'AGENDA DIGITALE ITALIANA

all'interno dell'ente: organigramma privacy. Tra i compiti specifici del DPO, l'art. 39 co. 1 lett. b) del GDPR menziona "... l'attribuzione delle responsabilità". Occorre dunque che il DPO valuti un corretto organigramma privacy che consenta di attribuire le responsabilità di ciascuno dei soggetti autorizzati al trattamento. Il DPO ha, quindi, il compito di assistere il Titolare in tale attività verificando, ad esempio, che tutti i nuovi assunti abbiano tempestivamente ricevuto tutte le necessarie istruzioni operative ai sensi dell'art. 29 del GDPR. Le verifiche citate sono solo una piccola parte dei controlli che il DPO è tenuto a svolgere con cadenza periodica nella sua attività di sorveglianza, madimostrano come sia arrivato il momento in cui il Data Pioneers Officer prenda in seria considerazione un diverso approccio metodologico fondato sulla capacità di standardizzare un sistema di controlli puntuale e in grado di dimostrare all'Autorità, nell'ottica del principio di accountability, di aver adeguatamente svolto i compiti previsti dall'art. 39 del GDPR. @RIPRODUZIONE RISERVATA