

Spett.le ORDINE DEI PERITI INDUSTRIALI  
E DEI PERITI INDUSTRIALI LAUREATI  
DELLE PROVINCE DI MILANO E LODI

alla c.a. del Presidente  
e del Consiglio Direttivo

## **RELAZIONE ANNUALE DEL RESPONSABILE DELLA PROTEZIONE DATI PERSONALI (DPO)**

Le attività di verifica ed audit, oltre a costituire un obbligo per i DPO (Data Protection Office e di seguito RPD), sono uno strumento di accountability (responsabilizzazione) per tutti i titolari e responsabili del trattamento.

Il GDPR prevede, quale mezzo principale per mettere in pratica il principio di responsabilizzazione, oltre alla nomina del Responsabile della protezione dei dati (RPD) anche:

- la creazione di un documento che indichi il tipo di dati raccolti e le finalità;
- l'identificazione di principi di minimizzazione dei dati in relazione alle differenti situazioni (solo i dati indispensabili, necessari e pertinenti);
- verificarne esattezza e conformità, oltre ad aggiornamento;
- proteggerne la conservazione e limitarla nel tempo;
- salvaguardarne integrità e sicurezza attraverso l'individuazione di procedure, formazione dei responsabili del trattamento e strumenti di protezione elettronici.

In relazione a ciò, durante l'anno in corso, la sottoscritta Monica Barreca **ha verificato con i Responsabili dei Trattamento, la Segreteria dell'Ordine, la correttezza e la congruità della documentazione, ha supportato il Titolare del Trattamento e i suoi delegati** ( Resp. Prevenzione Corruzione e Trasparenza, Referente Privacy, Resp. Sito web, Consiglieri delegati ad attività specifiche) **nella revisione del Registro dei Trattamenti e della modulistica dell'Ordine nella quale vengono raccolti dati personali.**

A tutela degli interessati sono state testate a campione alcune delle procedure manuali e/o elettroniche di raccolta e archiviazione dei dati, per verificare gli strumenti di protezione in atto. Tutte le verifiche hanno mostrato che **le procedure in attuazione presso l'Ordine risultano sufficienti a garantire la protezione della privacy degli interessati** e il personale addetto (Responsabili dei dati) correttamente formato in merito alla normativa e al rispetto dei processi interni.

L'Ordine anche durante l'anno in corso ha raccolto i dati personali degli interessati esclusivamente per finalità connesse alla natura e alle funzioni dell'Ordine, ovvero per finalità istituzionali di iscrizione al registro dei praticanti, iscrizioni all'albo e praticantato.

Durante l'anno in corso non sono state effettuate richieste di accesso civico che potessero comportare la registrazione dei dati personali dei richiedenti.

E' stata anche verificata l'esistenza di una procedura di aggiornamento dei dati, che rimette ai titolari l'onere/diritto di dare comunicazione alla segreteria di eventuali cambiamenti nonché aggiornamenti.

In relazione al principio di minimizzazione sono state prese in esame le procedure attraverso le quali l'Ordine raccoglie ed elabora i dati personali degli interessati e ove possibile sono state riviste, limitando la richiesta dei documenti e dati (per esempio utilizzando l'autocertificazione dei dati personali ed evitando di allegare il documento di identità). E' stata pertanto **rivista parte della modulistica in uso all'Ordine e pubblicata sul sito istituzionale**.

Il DPO concorda con il Titolare del Trattamento che a seguito delle valutazioni dei rischi per i diritti e le libertà delle persone fisiche derivanti da tali trattamenti che possano comportare un "rischio elevato", non appare necessario produrre, per l'anno in corso, il documento di Valutazione d'Impatto (DPIA).

In data 02/07/20 la Società QualiPer Srl, controllata dall'Ordine, ha subito un'intrusione informatica sul sito web. Tale intrusione non ha comportato alcuna violazione dei dati personali e quindi non è stato comunicato alcun data breach all'Autorità Garante, ma solo segnalazione alla Polizia Postale. Poichè gli addetti QualiPer svolgono mansioni di segreteria per l'Ordine, è stato necessario verificare la consistenza del sito web dell'Ordine, che le caselle mail degli addetti non avessero scaricato malware o si fossero installati nel computer della rete scraper.

Immediatamente è stata fatta una verifica sul sito che è risultato virus-free (mail Getmoon del 10/07/20) e richiesta assistenza di controllo direttamente al provider di servizi hosting Register (mail Register 14/10/20); successivamente è stato attivato specifico firewall di protezione del sito web SiteLock in versione Premium che prevede anche un motore di identificazione e rimozione automatica di malware.

Per maggiore sicurezza l'Ordine, attraverso la sua controllata QualiPer, ha attivato uno specifico contratto di servizi con la società Vertigo, che prevede lo spostamento dei siti web dell'Ordine e di QualiPer su un server virtuale dedicato per l'hosting. Si allegano tutti i documenti relativi alla pratica di cui sopra.\*

Il DPO attesta che per l'anno in corso **non sono occorse violazioni dei dati personali** e che **l'Ordine ha attivato adeguate misure di sicurezza, di natura "fisica" e "informatica"**:

Dal punto di vista della sicurezza fisica, i dati personali degli interessati sono conservati in appositi raccoglitori contenuti in armadi chiusi con serratura, le password di accesso al sistema vengono sostituite trimestralmente e conservate in contenitori di sicurezza anonimi, gli incaricati (sotto-responsabili dei dati) sono istruiti dai Responsabili circa le condotte da dover rispettare per garantire la tutela della riservatezza degli interessati e viene svolta periodica formazione e verifica del rispetto di tali indicazioni.

Inoltre gli atti e i documenti contenenti informazioni personali, sia in formato cartaceo che elettronico, sono presidiati e custoditi in modo tale che ad essi non possano accedere persone prive di autorizzazione e l'accesso agli archivi è possibile e limitato solo da parte di persone autorizzate.

La conservazione dei dati personali è coerente con i fini della raccolta e non ecceda i termini di legge o i criteri di conservazione temporale definiti dal Titolare in relazione ai termini di legge in adempimento al Regolamento sulla Privacy.

Al fine di prevenire rischi connessi all'utilizzo dei sistemi informatici di gestione dei dati, sono stati coinvolti nelle verifiche anche gli outsourcer e l'amministratore di sistema.

Benchè la normativa sia particolarmente articolata, vasta, trasversale e in continua evoluzione, il DPO, analizzati i trattamenti svolti, non ha rilevato difformità in relazione al GDPR e pertanto non sono state adottate misure correttive rilevanti da essere indicate nel registro.

Si ritiene comunque di fondamentale importanza per garantire sia gli interessati che l'Ordine stesso, **assistere puntualmente il Titolare del Trattamento nella verifica di nuove procedure e documenti e verificare con i Responsabili (segreteria) interventi formativi periodici volti a favorire la correttezza dell'implementazione di tutte le misure di sicurezza e l'applicazione puntuale del Regolamento.**

### **Raccomandazioni del DPO per l'anno 2021:**

Considerando che le violazioni (data breach) avvengono per i seguenti motivi [Data Breach Investigation Report 2020 by Verizon]:

1. **45% Hacking:** la causa principale è dovuta all'azione di hacker, che provano a rubare le credenziali di accesso ai sistemi aziendali: le trovano sul dark web, le trovano scritte negli uffici, oppure usano dei software per la generazione automatica di password.
2. **22% Errore umano:** anche l'errore di un impiegato può portare a una violazione delle informazioni.. per esempio inviare la mail alla persona sbagliata, con i dati sensibili di un'altra.
3. **22% Social engineering:** il phishing è l'invio di email che sembrano all'apparenza identiche a quelle di aziende importanti (pensiamo alle Poste), che richiedono spesso agli utenti di ripristinare i dati del proprio account. In realtà i destinatari accedono a dei portali fasulli, inviando involontariamente le proprie informazioni.
4. **17% Malware:** Strettamente legati alle attività dei cyber criminali, i malware possono essere utilizzati per numerose attività illecite. Un esempio di malware è il cosiddetto RAM Scraper (che scansionano la memoria dei dispositivi digitali per raccogliere informazioni sensibili) oppure ransomware, che bloccano i dispositivi elettronici chiedendo un riscatto.
5. **8% Accesso illecito dai dipendenti:** spesso alcuni utenti hanno la possibilità di accedere ai dati dei propri colleghi, perché magari hanno un account con accesso privilegiato o gestiscono processi amministrativi o fiscali.. a volte la violazione può essere semplicemente accidentale.
6. **4% Azioni fisiche:** dimenticare documenti con dati personali sulla scrivania con libero accesso, non distruggere accuratamente stampati contenenti dati personali, scordare di chiudere la serratura di armadi e cassetti d'archivio..

avendo verificato, come sopra espresso, che le misure richieste dal GDPR sono state adeguatamente implementate, il DPO consiglia per il 2021, l'attivazione delle seguenti procedure di sicurezza:

- a) **verificare il livello di attenzione relativamente ai rischi connessi all'utilizzo di sistemi informatici e violazioni ai dati tramite accessi fraudolenti dal web o dalla posta elettronica:**
  - nel primo semestre 2020 (rispetto al 2019) il numero totale di segnalazioni relative a ransomware (software malevoli che limitano l'accesso del dispositivo che infettano, richiedendo un riscatto da pagare per rimuovere la limitazione) è aumentato del 715,08%,
  - il numero totale di segnalazioni relative agli exploit (programmi dannosi contengono dati o codici eseguibili in grado di sfruttare una o più vulnerabilità di un software presente su computer locale o in remoto) è stato quattro volte superiore a quello del primo semestre del 2019 segnando un +405,79%;

- b) **incaricare formalmente un Responsabile Interno della Sicurezza Informatica** (ad. esempio un Consigliere) che provveda a verificare periodicamente lo stato di vulnerabilità/sicurezza del sistema e dell'attuazione da parte degli addetti di tutte le procedure di sicurezza, considerando che attualmente i data breach segnalati risultano avere origine per oltre l'80% da intrusioni informatiche.

Tale figura dovrebbe collaborare con la figura esterna dell'**amministratore di sistema**, il cui compito dovrebbe essere quello di verificare l'adeguatezza dell'apparato informatico e suggerire possibili implementazioni per ridurre i fattori di rischio e pericolo connessi all'utilizzo di sistemi informatici. **Si suggerisce pertanto al Responsabile Interno della Sicurezza Informatica e al Titolare del trattamento di esaminare con attenzione tutti i report rilasciati dall'amministratore di sistema adottando i correttivi eventualmente suggeriti da part di quest'ultimo.** Contestualmente si invitano il Titolare e il Responsabile a sollecitare all'amministratore di sistema la massima attenzione e cura nella redazione dei propri report in modo tale da poter avere contezza dei rischi connessi ai trattamenti svolti mediante strumenti elettronici e se del caso pianificare i necessari correttivi.

- c) **Utilizzare applicazioni software, plugin, web application adeguatamente** aggiornate e verificare la potenziale vulnerabilità dei sistemi in uso *(es. web app ZOOM vs. 4.6: è stata scoperta una vulnerabilità di Zoom che consente di iniettare codice malevolo nell'app di videoconferenze e registrare le riunioni e le chat a totale insaputa dei partecipanti, anche se sono attive tutte le funzioni di sicurezza dell'applicazione. Tale malware si attiva anche con firewall attivo e telecamera off)*
- d) **Modificare trimestralmente le password di accesso alle caselle di posta elettronica e ai sistemi gestionali dell'Ordine** *(La password deve essere composta da almeno 8 caratteri, deve contenere almeno un carattere appartenente alle lettere maiuscole (da A a Z), deve contenere almeno un carattere appartenente ai primi 10 numeri di base (da 0 a 9), deve contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !, \$, #, %), deve essere diversa da quella precedente (quella cioè rilasciata dall'Amministratore), evitare di cliccare link presenti nelle email e verificare periodicamente se il proprio account mail è stato compromesso in un data breach (per es. attraverso il link <https://haveibeenpwned.com>)).*

L'email è il principale vettore di minacce che i criminali informatici utilizzano per sferrare un attacco informatico o perpetrare una truffa per raccogliere informazioni sensibili relative agli utenti. In particolare, gli spammer hanno affinato le loro competenze nel corso dell'ultimo anno, sviluppando email che spesso eludono gli algoritmi di filtraggio dello spam e i sistemi di analisi.

- e) **Individuare i preposti coinvolti in attività di trattamento facendo in modo che siano formalmente incaricati** e autorizzati da parte del Titolare; siano adeguatamente responsabilizzati e ricevano idonee istruzioni in modo tale che rispettino le prescrizioni di legge vigilando su di essi affinché siano osservate le disposizioni e le istruzioni impartite. Per quanto concerne le persone coinvolte nell'attività di trattamento si suggerisce di compiere con costanza un'analisi di quali possano essere i soggetti autorizzati al trattamento assegnando loro un documento di incarico integrato con idonee istruzioni e programmare **interventi formativi** nei confronti di tutto il personale addetto e i Responsabili designati
- f) **Favorire l'elaborazione di best practice, intervistando gli addetti al trattamento circa** problematiche riscontrate nelle attività quotidiana, potenziali rischi fronteggiati, modalità operative e richieste/domande da parte degli interessati.
- g) Nel merito delle **attività delegate a soggetti esterni**, come indicato dall'art 28 del Regolamento, si invita voler verificare quali siano i rapporti in essere oltre quelli già oggetto di ricognizione negli scorsi mesi in modo tale da formalizzare nei confronti dei soggetti che compiono operazioni per conto del titolare (es. Responsabile Paghe, Commercialista, Avvocato, Resp. Sicurezza,...) idonei atti di nomina con la definizione della natura, della durata e delle finalità dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento. Appare utile ricordare che nei confronti dei responsabili si dovrà sollecitare il rilascio di una copia del registro dei trattamenti previsto dall'art. 30, II comma del Regolamento.

Si allega alla presente la documentazione vistata dal DPO, rivista con il Titolare del Trattamento:

- registro dei trattamenti di dati personali;
- \*documentazione relativa alle verifiche di vulnerabilità del sito web e allo spostamento dei siti su server dedicati

Si ringrazia per l'attenzione e si ribadisce la disponibilità per ogni necessario chiarimento.

Trento, 30 novembre 2020

Il DPO

Monica Barreca

