Responsabile della Protezione dei Dati Personali

EXECUTIVE SUMMARY

AUDIT DI SINTESI GENNAIO 2019

ACER PROVINCIA DI RIMINI

ACER
Azienda Casa Emilia-Romagna

AREA LEGALE – ORGANIZZAZIONE – ICT

Data audit	15 gennaio 2019
Data redazione	24 marzo 2019
Auditor/s AP&P srl	Silvia Dalle Nogare – Roberto Ballanti – Vittordavide Frison
Nome del file	executivesummary.docx

SOMMARIO

1. CONTESTO E CONTENUTI

Il presente report si riferisce agli audit svolti presso le ACER di Rimini e Forlì-Cesena (in data 15/01/2019) e di Ravenna e Ferrara (in data 16/01/2019), nell'ambito dell'incarico di *Responsabile della protezione dei dati – RPD, ai sensi degli art. 37 – 38 – 39 del GDPR,* sottoscritto fra le suddette ACER e la società AP & Partners srl.

Trattandosi del primo atto di intervento formale del RPD, gli audit hanno avuto ad oggetto l'esame preliminare degli adempimenti posti in essere da ciascun Ente per l'adeguamento al Regolamento UE 679/2016, per brevità anche RGPD, e al D.lgs. 196/2003 Codice Privacy (come modificato/abrogato dal D.lgs. 101/2018) in ambito legale-organizzativo e tecnico (ossia relativo alle infrastrutture informatiche e telematiche dell'Ente).

A seguito delle attività di audit sono state generate e consegnate a ciascuna ACER i rispettivi riepiloghi delle evidenze raccolte e segnalato quelle che hanno un maggiore impatto e rischio sulla protezione dei dati personali.

1.1 Area legale – organizzativa

Le attività di verifica, svolte secondo un approccio collaborativo e di supporto al Titolare del trattamento, si sono concentrate sull'esame a campione dei documenti e delle procedure (finalizzate o in corso di approvazione) nonché sull'analisi delle macro criticità inerenti all'ambito legale-organizzativo, al fine di evidenziare possibili azioni migliorative e strutturare la seconda fase di verifica che avrà ad oggetto i singoli adempimenti e/o l'attuazione del piano di miglioramento suggerito.

Nello specifico delle attività di questa area, sono state prese in esame i seguenti aspetti:

- Liceità del trattamento;
- Informativa e consenso;
- Diritti dei soggetti interessati;
- Ruoli privacy;
- Registro delle attività di trattamento;
- Conformità sito web.

Dall'audit sono state formalizzate n° 15 azioni di miglioramento.

1.2 Area Ict

Lo scopo primario della presente analisi, nella specifica area Ict, è quello di permettere ai vertici dell'Ente e a chi non ha competenze informatiche, di percepire le criticità presenti sul sistema informativo e di poter provvedere ad eseguire una serie di azioni, in conseguenza della gestione del rischio rilevata, che permettano di proteggere adeguatamente il patrimonio informativo aziendale.

Gli obiettivi generali dell'analisi, nella specifica area Ict, sono i seguenti:

- comprendere come l'insieme delle informazioni sia strutturato (informazioni soggette a Confidenzialità o a prescrizioni connesse alla normativa privacy, etc.);
- individuare le aree di rischio per ogni macro-categoria definita;
- individuare la metodologia per la classificazione dei rischi insistenti su ogni area;
- proporre delle ipotesi operative per il contenimento dei rischi rilevati;
- delimitare l'area sulla quale non verrà operata l'attività di analisi (motivando la scelta);
- cercare di allineare le ACER soggette a verifica ad un insieme di prassi, procedure e comportamenti omogenei per garantire la sicurezza delle informazioni.

Andando ad effettuare una verifica, sempre sulla base delle attività d'intervista condotte con gli amministratori di sistema (per brevità anche ADS) ed i responsabili dei vari procedimenti, si è reso necessario suddividere il sistema informativo in ulteriori sottoinsiemi funzionali alle applicazioni/processi gestiti che sono:

1) Attività condotte dall'ADS;
2) Rischio connesso agli strumenti (valutazione generale);
3) Comportamenti degli operatori;
4) NTP Server;
5) Tracciabilità degli eventi (Log);
6) SysLog Server;
7) Gestione della sicurezza (Firewalling e Antivirus);
8) Servizi esposti;
9) Tracciabilità degli incidenti;
10) Backup e Disaster Recovery;

Per ognuna delle voci sopra riportate si è provveduto ad effettuare una verifica che è stata condotta al fine di rilevare il grado di rischio e permettere di suggerire misure di mitigazione del rischio idonee.

Dall'audit sono state formalizzate n° 10 azioni di miglioramento.

2. RIFERIMENTI NORMATIVI E DOCUMENTI DI RIFERIMENTO

Art 37 – Designazione del responsabile della protezione dei dati del RGPD;

Art. 38 – Posizione del responsabile della protezione dei dati del RGPD;

Art. 39 – Compiti del responsabile della protezione dei dati del RGPD.

ISO/IEC 27001:2013 Information Security Management Systems;

ISO/IEC 27002:2013 Code of practice for information security controls;

EEN-IT PO02 Information system security policy;

D.lgs. 196/03 e s.m.i. – Codice in materia di protezione dei dati personali o Codice Privacy, come modificato dal D.lgs. 101/2018;

Regolamento UE 679/2016 di seguito denominato RGPD;

L.R. 24/2001 – Disciplina generale dell'intervento pubblico nel settore abitativo;

D.lgs. 231/01 e s.m.i. – Responsabilità amministrativa delle società e degli enti;

Provvedimento "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"

BEST PRACTICES NIST E SANS.

Allegati:

- Report audit di sintesi gennaio 2019;
- Check – list audit area Legale – Organizzazione;
- Cookie scan report;
- Determinazione dell'ambito di applicazione dell'analisi del rischio sulla sicurezza delle informazioni.

Rimanendo a disposizione per eventuali chiarimenti, porgiamo i più distinti saluti.

Ferrara, 24/03/2019

Team Rpd:

(Rpd: Roberto Ballanti) (Silvia Dalle Nogare) (Vittordavide Frison)