Lamezia Terme, 18/08/2020

Spett.le
CARBOSULCIS SPA
Località Monte Sinni (Nuraxi Figus)
09010 Gonnesa (Carbona-Iglesias/CI) – Sardegna/Italy

alla c.a. del *Dott. Massimiliano Vacca*
E-mail: vacca.massimiliano@carbosulcis.eu

E p.c.

Alla c.a. dell'*Ing. Elisabetta Fois*
E-mail: fois.elisabetta@carbosulcis.eu;

Alla c.a. dell'Amministratore di Sistema *Sig. Giorgio Scussel*
E-mail: scussel.giorgio@carbosulcis.eu;

- *Trasmesso via Mail*

➢ PROT. N° 1858

OGGETTO: Definizione procedura gestione "Data Breach", accordi di contitolarità e mappatura Responsabili del trattamento, ai sensi del Regolamento Europeo 679/2016 ("GDPR") e del D.Lgs. 196/2003 e ss.mm.ii. (D.Lgs. 101/2018)

In riscontro all'incarico di Responsabile della Protezione dei Dati/Data Protection Officer – RPD/DPO affidatoci e dei servizi di supporto all'attuazione del Regolamento Europeo 679/2016, finalizzato a garantire l'adeguamento (*c.d. "Compliance"*) della Vostra Società all'attuale normativa (*giusto Ordine di Acquisto n. O/143/19, giusto Contratto SE0013/19343 – prot. carbspa 0002601 del 18/12/2019 sottoscritto da entrambe le parti*), e facendo seguito all'Audit svolto presso la Vs sede e ai cordiali contatti intercorsi, si trasmettono i seguenti documenti come di seguito descritti:

DATA BREACH POLICY_Disposizioni operative in materia di incidenti di sicurezza e di violazione di dati personali:

Si trasmette la policy/disciplinare da adottare al fine di contenere e gestire al meglio gli eventuali incidenti di sicurezza e violazioni che potranno avvenire nell'azienda. Unitamente a tale policy sono presenti gli allegati che ne formano parte integrante e che andranno messi a disposizione di tutti gli interessati. Tra cui:

- **Allegato A - "Modulo di segnalazione di una potenziale violazione di dati personali":** Tale modulo, da pubblicare sul sito web nell'apposita sezione dedicata alla "privacy", è messo a disposizione di tutti quei soggetti che non sono legati al Titolare del trattamento da rapporti contrattuali/vincolanti, ma che vogliono segnalare eventuali anomalie, disservizi o potenziali incidenti sulla sicurezza;
- **Allegato B - "Modulo di inoltro di segnalazione di una potenziale violazione di dati":** Tale modulo serve, una volta ricevuta la segnalazione da un soggetto non legato al Titolare del trattamento da rapporti contrattuali/vincolanti (attraverso il precedente allegato A), per inoltrarla al Titolare del trattamento o a un Designato competente in ragione del servizio o settore/area/ufficio coinvolto, senza ritardo e, comunque, entro 4 ore dalla sua ricezione. Tale modulo va anche pubblicato sul sito, poichè deve essere reso disponibile a tutti i soggetti legati al Titolare. N.B.: Ovviamente nel caso la segnalazione arrivi da un soggetto interno al Titolare non sarà necessario effettuare questo doppio "passaggio".
- **Allegato C - "Modulo di valutazione del rischio connesso al violazione di dati personali":** Acquisito un ragionevole grado di certezza che sia avvenuto un incidente per la sicurezza delle informazioni che abbia compromesso dei dati personali, il Designato competente deve stimare la gravità e la probabilità della violazione e classificare il rischio, e documentare la decisione presa a seguito della valutazione nel Registro delle violazioni. Gli elementi e gli esiti della valutazione sono documentati utilizzando appunto il presente modello Allegato C. Tale modello "vuoto" va pubblicato sul sito web.
- **Allegato D – "Violazione di dati personali – modello di notifica al Garante":** Tale modello è utilizzato per notificare le violazioni all'Autorità di controllo, previa consultazione ed in collaborazione con il DPO. Tale modello "vuoto" è consigliato pubblicarlo sul sito web.

- **Allegato E – "Comunicazione all'interessato della violazione dei dati personali":** Tale modello è utilizzato nel caso di accertamento di una violazione di dati personali che sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, quindi per informare i singoli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio (qualora in numero degli interessati sia "ridotto"). Anche tale modello "vuoto" è consigliato pubblicarlo sul sito web.
- **Allegato RDB_Registro Data Breach:** In tale registro vanno annotate tutte le violazioni/incidenti di sicurezza (anche quelle non notificate al Garante). Non va pubblicato sul sito web.
- **Allegato F - "Accordo di contitolarità":** Tale modello va utilizzato/"siglato" laddove il Titolare si trovasse ad operare unitamente ad altri soggetti per il trattamento di dati personali. Non è obbligatorio pubblicarlo sul sito web.
- **Allegato G - "Appendice contrattuale/Responsabile del trattamento":** laddove il Titolare necessiti che il trattamento di dati personali venga effettuato per suo conto ad opera di altri soggetti esterni, qualificabili appunto come Responsabili del trattamento, quindi quando viene esternalizzato un servizio che richiede il trattamento di dati personali per conto del Titolare (ad esempio esternalizzazione servizio paghe, ricerca e gestione del personale, ecc). * Con tale Appendice contrattuale/nomina si "richiede" al Fornitore (quindi al Responsabile del trattamento, che ricordo è solo ed esclusivamente un soggetto esterno) di sottoscrivere per presa visione l'atto di designazione contenente i vincoli, gli ambiti del trattamento nonché gli obblighi da rispettare nel trattamento stesso dei dati, per l'espletamento dei servizi da effettuare per conto del Titolare. Quindi la sottoscrizione da parte del fornitore non è un'accettazione (perché nel momento in cui viene affidato un servizio che richiede un trattamento di dati per conto del Titolare, questi fornitori sono individuati dalla stessa normativa Responsabili del trattamento), ragion per cui si raccomanda ove non assolto a monte, la trasmissione mezzo PEC (così da avere una tracciabilità e poterne dimostrare la trasmissione).
- **Allegato R.I_Registro-elenco Responsabili del trattamento:** è fondamentale che si tenga traccia di tali Responsabili del trattamento, ragion per cui a seguito di ogni affidamento che comporti un trattamento di dati personali esternalizzati, è necessario redigere e tenere aggiornato un elenco di tali responsabili. Ho predisposto per Voi un Registro/Elenco da

aggiornare (può essere unico quindi salvato in una cartella condivisa da tutti i settori/uffici, oppure compilato e tenuto da ognuno). Per facilitarvi il lavoro, ho creato un format già personalizzato;

- **Allegato R.2_Modello richiesta informazioni Responsabili del trattamento:** Inoltre, il Titolare ha la possibilità/facoltà di effettuare audit/ispezioni e/o richiedere a tali Responsabili, durante lo svolgimento dei servizi, informazioni circa i trattamenti/le misure di sicurezza adottate, ecc. Sempre per facilitarvi il lavoro, ho predisposto un format che potrete utilizzare qualora ne riscontriate l'esigenza.

Ovviamente sia l'adozione che la spiegazione della policy e della presente modulistica verrà affrontata nell'Audit che si terrà presso la Vs sede a fine settembre. Inoltre anche nel proseguo, nella la ricezione delle segnalazioni, nell'aggiornamento dei registri e nelle valutazioni dei rischi, nonché nelle eventuali comunicazioni all'autorità Garante la Scrivente vi seguirà passo dopo passo negli adempimenti.

In attesa di Vs riscontro e conferma per i giorni dal 21 al 25 settembre degli Audit, si resta a completa disposizione per eventuali chiarimenti, invitandoVi a contattarci in qualsiasi momento.

per Multibusiness Srl

Data Protection Officer
Dott. Pasquale Nicolazzo

RIFERIMENTI

Dott. Pasquale Nicolazzo, 320.9585082
Tel: 0968.462702 – Fax: 0968.464273
E-mail: p.nicolazzo@garanteprivacyitalia.it
PEC: info@pec.garanteprivacyitalia.it
Portale web: www.garanteprivacyitalia.it