

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI DI BIELLA

Via Duomo, 3
13900 BIELLA (BI)
Tel: 01533619
C.F. 90054690020



ORDINE DEI DOTTORI COMMERCIALISTI
E DEGLI ESPERTI CONTABILI DI BIELLA

DATA PROTECTION IMPACT ASSESSMENT - Ai sensi art. 35 del Regolamento Europeo 2016/679

Scopo di questo documento è di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, adottate e da adottare per il trattamento dei dati personali effettuato da ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI DI BIELLA per una valutazione dell'impatto sui trattamenti.

Misure Logiche e Organizzative

Le seguenti misure organizzative sono da considerarsi su tutta l'organizzazione Aziendale

Misure Adottate

- ▶ Descrizione scritta degli interventi effettuati da terzi.
- ▶ Redazione del Registro dei Trattamenti sia in qualità di Titolare sia se necessario in qualità di Responsabile
- ▶ Redazione documento Privacy by Design e By Default
- ▶ Nomina del DPO
- ▶ Procedure Gestione Data Breach
- ▶ Implementazione Procedura di Nomina a Responsabile del trattamento
- ▶ Verifica delle valutazioni preventive ai sensi dell'art. 5 paragrafo 1 del GDPR.
- ▶ Redazione di un piano di formazione per gli addetti
- ▶ Verifica periodica dell'ambito dei trattamenti e dei profili di autorizzazione.
- ▶ Verifica dei Back-up.
- ▶ Consegna istruzioni dettagliate agli addetti.
 - Istruzioni per la segretezza del sistema di autenticazione e la custodia dei dispositivi personali.
 - Istruzioni sulla custodia degli strumenti elettronici durante le sessioni di trattamento.
 - Istruzioni per i supporti removibili in caso di dati sensibili o giudiziari.
 - Istruzioni scritte finalizzate al controllo ed alla custodia dei documenti cartacei.
- ▶ Procedure per ripristino dei dati.
- ▶ Distruzione dei supporti removibili.

Elenco per trattamento

I rischi associati ai trattamenti sono la somma pesate dei rischi logici ed organizzativi sui dati e dei rischi presenti sugli archivi utilizzati per il trattamento.

• Gestione segnalazioni Whistleblowing

Fattore di rischio residuo dopo valutazione di impatto **3/10** (Basso)

Gestione segnalazioni Whistleblowing

Livello di copertura:

- Fattore di rischio iniziale: 8/10
- Fattore di rischio residuo: 3/10
- Percentuale di copertura tramite misure attuate: 65%
- Percentuale di copertura tramite misure da attuare dopo valutazione di impatto: 65%

Dati Comuni trattati:

- nominativo, indirizzo o altri elementi di identificazione personale.

Dati Particolari trattati:

- Dati comuni ed eventuali dati particolari trattati nell'ambito della gestione delle segnalazioni whistleblowing.

Archivi utilizzati per il trattamento

- whistleblowing.it .

Interessati al trattamento, finalità e base giuridica

► Segnalante whistleblowing

- rivelazione della sua identità a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni (comma 2 dell'art. 12 D.Lgs 24/2023) o nell'ambito del procedimento, ove la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza della sua identità sia indispensabile per la difesa dell'incolpato (comma 5 dell'art. 12 D.Lgs 24/2023). [richiesta di consenso].
- Attività di compliance in ambito D.Lgs 24/2023 [obbligo di legge o contrattuale].
- Ricezione, analisi e gestione della segnalazione, nonché per l'accertamento dei fatti oggetto della stessa e adozione dei conseguenti provvedimenti, in adempimento delle previsioni di cui al D. Lgs. 10 marzo 2023, n. 24 [obbligo di legge o contrattuale].

Rischio di Disponibilità dei dati

► Eliminazione o perdita dei dati al di fuori dell'ambito definito

Rischio Residuo **MOLTO BASSO**
Livello di Copertura **MOLTO ALTO**

► Mancata disponibilità dei dati

Rischio Residuo **MOLTO BASSO**
Livello di Copertura **MOLTO ALTO**

Rischio di Integrità dei dati

► Modifica errata o mancato aggiornamento dei dati

Rischio Residuo **MOLTO BASSO**
Livello di Copertura **MOLTO ALTO**

► Trattamento dei dati secondo modalità differenti da quelle dichiarate

Rischio Residuo **MOLTO BASSO**
Livello di Copertura **MOLTO ALTO**

Rischio di Riservatezza dei dati

▶ Diffusione dei dati al di fuori dell'ambito definito	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
▶ Comunicazione dei dati al di fuori dell'ambito definito	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
▶ Trattamento dei dati al di fuori dell'ambito degli addetti autorizzati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO

Accadimenti possibili sugli archivi

Fault o malfunzionamento della strumentazione IT	Rischio Residuo	ALTO
	Livello di Copertura	MOLTO BASSO
Eccesso di traffico sulle linee di TLC	Rischio Residuo	MEDIO
	Livello di Copertura	MOLTO BASSO
Danni alle linee di TLC	Rischio Residuo	MEDIO
	Livello di Copertura	BASSO
Distruzione o Modifica volontaria dei Dati	Rischio Residuo	BASSO
	Livello di Copertura	MEDIO
Distruzione di strumentazione da parte di persone malevole	Rischio Residuo	BASSO
	Livello di Copertura	BASSO
Divulgazione Intenzionale dei Dati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MEDIO
Errori di trasmissione (incluso il misrouting)	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	BASSO
Errori di manutenzione hardware e software	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	ALTO
Furti di Dati perpetrati dall'esterno	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Errori non volontari durante modifica o cancellazione di Dati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Accesso non autorizzato o Furto di dati personali	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	ALTO
Distruzione o Modifica accidentale dei Dati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Divulgazione accidentale dei Dati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO

Accesso a Sistemi contenenti informazione da parte di addetti non autorizzati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Saturazione dei sistemi IT	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Errore di salvataggio sui supporti di Back-up	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Furti di Dati perpetrati da personale Interno	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Presenza di Virus	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Scrittura Dati errati	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Furto di Identità degli Addetti	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Mancato recupero di informazioni da media (principalmente memorie di massa) di backup up	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Furto di apparati o sistemi	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO
Malfunzionamenti software	Rischio Residuo	MOLTO BASSO
	Livello di Copertura	MOLTO ALTO

Misure Adottate

Misure Fisiche

- ▶ **Credenziali di autenticazione, assegnate individualmente ad ogni addetto.**
 - Autenticazione mediante user-id e password.
 - Parola chiave di almeno 8 caratteri.
 - Disattivazione delle vecchie credenziali.
 - Disposizioni scritte per la disponibilità dei dati.
- ▶ **Cifratura dei dati memorizzati.**
- ▶ **Cifratura dei dati trasmessi.**
 - Cifratura con protocollo SSL.
- ▶ **Sospensione automatica delle sessioni di lavoro.**
- ▶ **Sospensione manuale delle sessioni di Lavoro.**
- ▶ **Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.**
- ▶ **Pseudonimizzazione.**
- ▶ **Profili di autorizzazione di ambito diverso per diversi incaricati.**
- ▶ **Separazione Fisica delle copie dei dati.**

Misure previste dal piano di mitigazione dei Rischi

Nessuna