Misure di natura tecnica e organizzativa secondo l'art 32 del GDPR

Informazioni sul documento	
Versione	1.0
Data	07/02/2019
Classificazione dei documenti	Pubblico
Stato di approvazione	Approvato
Versione originale rilasciata da	Responsabile della privacy di 1&1
Versione attuale rilasciata da	Responsabile della privacy del gruppo United Internet AG
Rilasciato il	07/02/2019

Indicazioni

Il presente documento contiene informazioni che vengono messe a disposizione di partner commerciali, clienti e altri soggetti esterni che godono di diritto di ispezione legale o di altro diritto di ispezione giustificato.

Per motivi di leggibilità, nel testo viene utilizzata la forma maschile, tuttavia le informazioni si riferiscono a membri di entrambi i sessi.

Preambolo

Il responsabile ha attuato misure consone in materia di riservatezza, integrità, disponibilità e resistenza, nonché procedure regolari di verifica e valutazione.

La parte generale descrive le misure tecniche e organizzative che si applicano indipendentemente dai rispettivi servizi, sedi e clienti. Negli allegati vengono descritte misure che si applicano al di là delle misure documentate nella parte generale.

1. Riservatezza

Riservatezza significa che i dati personali non vengono resi disponibili o divulgati a persone, entità o processi non autorizzati.

Controllo ingresso

- Servizio di reception e di sicurezza
- Autorizzazioni individuali, documentate e dipendenti dal ruolo (carte, transponder e chiavi) per l'ingresso nell'edificio
- Pass per dipendenti e visitatori
- I visitatori possono entrare nell'edificio solo se accompagnati da un dipendente
- Sistema di allarme e antifurto
- Gli uffici vengono chiusi a chiave al di fuori dell'orario di lavoro

Controllo login

- Procedure utente e di autorizzazione formali
- Login solo con nome utente, password e, se richiesto, autenticazione a 2 fattori
- Politiche sulle password applicate in modo sistematico
- VPN per accessi remoti e tramite dispositivi gestiti dal responsabile
- Mobile Device Management
- I supporti dati mobili sono criptati
- Blocco automatico del desktop dopo pochi minuti di inattività
- Clean Desk-Policy

Controllo accesso

- Mantenimento dei registri degli attivi e derivazione delle misure sulla base della classificazione dei dati
- Utilizzo di procedure crittografiche (ad esempio, crittografia)
- Implementazione dei concetti di autorizzazione secondo il principio del Need-to-Know
- Separazione degli accessi applicativi e amministrativi
- Registrazione dei tentativi di accesso
- Impostazione delle stazioni di lavoro dell'amministratore
- Numero minimo di amministratori
- Utilizzo della distruzione di documenti

Pseudonimizzazione

- Se possibile o necessario, i dati personali vengono trattati con uno pseudonimo (separazione dei dati di assegnazione e memorizzazione in un sistema separato)

Controllo separazione

- Separazione dell'ambiente di sviluppo, di test e di produzione
- I dati personali non possono essere utilizzati per scopi di test

- Capacità client / separazione logica dei dati per le applicazioni rilevanti: database separati, separazione schematica nei database, concetti di autorizzazione e/o archiviazione di file strutturati

2. Integrità

L'integrità dei dati personali è preservata se i dati sono accurati, immutati e completi.

Controllo trasmissione

- Trasmissione di dati tramite connessioni criptate (ad es. SFTP)
- Divulgazione di dati personali in base ai principi Need-to-Know / Need-to-Do
- I dati personali vengono classificati in base alle loro esigenze di protezione, mentre i dati riservati possono essere trasmessi solo tramite canali di comunicazione sicuri
- Ove possibile, viene utilizzata la crittografia per la posta elettronica
- Ove possibile, i dati personali vengono trasmessi solo in forma pseudonimizzata o anonima
- Documentazione della distribuzione dei supporti fisici di archiviazione
- I documenti cartacei contenenti dati personali vengono trasmessi solo in una busta sigillata e opaca

Controllo immissioni

- Registrazione tecnica dell'immissione, della modifica e della cancellazione dei dati personali nonché del controllo dei registri
- Tracciabilità dell'immissione, della modifica e della cancellazione dei dati da parte dei singoli nomi utente (non dei gruppi di utenti)
- Concetto di autorizzazione basato sui ruoli (diritti di lettura, scrittura e cancellazione)
- Registrazione delle modifiche amministrative

3. Disponibilità e resistenza

La disponibilità dei dati personali viene garantita se i dati personali possono sempre essere utilizzati secondo le esigenze degli utenti

- Utilizzo di firewall hardware e software
- Sistemi di rilevamento delle intrusioni
- Protezione contro le sovratensioni del rivestimento esterno dell'edificio contro i fulmini
- Alimentazione elettrica ininterrotta (UPS)
- Manuali di emergenza per il recupero dei dati, per la tutela contro la distruzione o la perdita di dati accidentale
- Esecuzione di test di recupero
- Dove necessario, utilizzo di sistemi ridondanti (ad es. RAID)
- Verifica periodica del backup dei dati
- Audit esterni e test di sicurezza

4. Procedure periodiche di verifica e valutazione

In che modo viene garantito che le misure di protezione dei dati menzionate vengano riesaminate regolarmente?

Gestione della privacy

- Nomina di responsabili della privacy e un responsabile della sicurezza delle informazioni
- Istituzione di un'organizzazione per la privacy e la sicurezza delle informazioni
- Tutti i dipendenti sono tenuti a mantenere la riservatezza nel trattamento dei dati personali e sono a conoscenza della segretezza delle telecomunicazioni

- I dipendenti vengono sensibilizzati in merito al trattamento dei dati personali
- I nuovi dipendenti ricevono materiale informativo relativo al trattamento dei dati personali
- Viene tenuto un registro delle attività di trattamento dei dati e vengono effettuate, se necessario, valutazioni sull'impatto della privacy
- Sono state istituite procedure per l'esercizio dei diritti degli interessati

Controllo commissione

- I dati trattati per conto del cliente vengono trattati solo secondo le istruzioni del cliente
- I mandatari vengono accuratamente selezionati tenendo conto delle misure tecniche e organizzative per la protezione dei dati personali interessate
- Le istruzioni per il trattamento dei dati personali vengono documentate in forma scritta
- Se necessario, vengono conclusi accordi di trattamento o garanzie adeguate per il trasferimento di dati a paesi terzi

Impostazioni conformi alla privacy

- Si garantisce che i sistemi e i prodotti siano sviluppati in modo tale da garantire la protezione dei dati
- Vengono raccolti solo i dati personali che sono necessari al rispettivo scopo

Incident-Response-Management

- Processo documentato per individuare, segnalare e documentare le violazioni della privacy con il coinvolgimento del responsabile della privacy
- Procedura documentata per la gestione degli incidenti di sicurezza con la partecipazione del responsabile della sicurezza delle informazioni

Allegato 1: Misure tecniche e organizzative specifiche per i centri di calcolo

- Tutti i centri di calcolo sono certificati secondo la norma ISO 27001
- I sistemi elettronici di controllo degli accessi monitorano e garantiscono l'accesso ai centri di calcolo solo alle persone autorizzate
- Barriera/chiusa di sicurezza
- Le videocamere e i rivelatori antifurto e di contatto sorvegliano la pelle esterna dell'edificio
- Zone di sicurezza definite
- Infrastruttura di rete altamente ridondante
- Il rivelatore d'incendio e/o di fumo ha un collegamento diretto con i vigili del fuoco locali
- Sistema di raffreddamento nei centri di calcolo / sale server
- Monitoraggio della temperatura e dell'umidità delle sale server
- Nessun collegamento sanitario all'interno o all'esterno dei centri di calcolo
- Messaggio di allarme in caso di accesso non autorizzato ai centri di calcolo