Misure tecniche e organizzative

|  |  |  |
| --- | --- | --- |
| **No.** | **Categoria** | **Descrizione** |
| **0** | **Organizzazione** | |
|  | Come è organizzata l'attuazione della protezione dei dati? | Un responsabile esterno della protezione dei dati è nominato per svolgere le funzioni di consulenza e controllo ai sensi del GDPR. |
|  | Vi preghiamo di fornirci il nome e i dati di contatto del vostro responsabile della protezione dei dati. | Christian Volkmer Projekt 29 GmbH & Co. KG Ostengasse 14, 93047 Regensburg, GermaniaTel : +49 941 2986930E-Mail : c.volkmer@projekt29.de |
|  | In che modo i collaboratori vengono formati all'attuazione delle misure tecniche e organizzative concordate che vengono utilizzate per questa elaborazione? | Formazione regolare sulla protezione dei dati per tutti i dipendenti  Obbligo di tutti i collaboratori alla dichiarazione sulla protezione dei dati |
|  | Le procedure di trattamento sono documentate per quanto riguarda l'ammissibilità della legge sulla protezione dei dati? | Sì, i flussi di dati sono documentati nell'ambito del repertorio procedurale interno e l'ammissibilità dell'elaborazione e dell'utilizzo è dimostrata in conformità con il GDPR. |
| **1** | **Riservatezza (Art. 32 Abs. 1 lit. b GDPR)** | |
| **1.1** | **Controllo dell'accesso fisico** | |
|  | In che modo gli edifici in cui avviene il trattamento sono protetti da accessi non autorizzati? | Sistema di allarme in una parte dell'edificio dell'azienda. |
|  | Come sono protetti da accessi non autorizzati i locali / uffici in cui avviene il trattamento? | Circuiti fusibili del sistema di allarme. Accesso solo per i dipendenti tramite chip RFID dedicato.  Notifica del servizio di sicurezza e di alcuni dipendenti in caso di allarme. |
|  | Come sono protetti i sistemi di elaborazione contro l'accesso non autorizzato? | Circuito di sicurezza separato del sistema di allarme con accesso solo per il personale amministrativo. |
|  | Come si verifica l'idoneità delle misure di controllo degli accessi attuate? | Anche le misure di controllo dell'accesso sono controllate dal responsabile esterno della protezione dei dati nell'ambito dei controlli. |
| **1.2** | **Controllo accessi interno** | |
|  | Come vengono assegnati gli accessi utente? | I capi reparto o gli amministratori delegati segnalano all'amministrazione l'ingresso di nuovi collaboratori.  I dipendenti ricevono gli account Microsoft Active Directory (AD) al momento dell'iscrizione; le autorizzazioni sono controllate tramite i gruppi AD. (reparto, team o affiliati individuali) |
|  | Come viene controllata la validità degli accessi degli utenti? | I capi reparto o gli amministratori delegati sono tenuti a comunicare in tempo utile all'amministrazione qualsiasi cambiamento rilevante nei rapporti di lavoro. |
|  | Come vengono documentati gli accessi degli utenti, comprese le procedure di richiesta, approvazione, ecc. | Le richieste di accesso degli utenti possono essere richieste o approvate solo dai capi reparto o dagli amministratori delegati via e-mail e vengono confermate dall'amministrazione via e-mail. L'avanzamento viene registrato tramite l'archiviazione della posta. |
|  | Come si garantisce che il numero di accessi all'amministrazione sia ridotto esclusivamente al numero necessario e che a tal fine venga impiegato solo personale professionalmente e personalmente idoneo? | L'accesso all'amministrazione è concesso solo agli amministratori di sistema dedicati e ai sostituti, previa approvazione della direzione.  Tutte le persone interessate e aventi diritto hanno un comprovato background tecnico informatico con esperienza nell'amministrazione. Non sono né temporanei né impiegati come dipendenti esterni, non sono in periodo di prova e sono vincolati dalla politica sulla privacy dell'azienda. |
|  | L'accesso ai sistemi/applicazioni è possibile dall'esterno (home office, fornitori di servizi, ecc.) e come è strutturato l'accesso? | L'accesso è possibile tramite una connessione VPN criptata (L2TP) per i dipendenti esplicitamente autorizzati. L'identificazione viene effettuata tramite i dati di accesso di Microsoft Active Directory e una chiave pre-condivisa. |
| **1.3** | **Controllo elettronico degli accessi** | |
|  | Come si ottiene che le password siano note solo al rispettivo utente? | Non ci sono account utente condivisi.  Gli utenti ricevono una password iniziale individuale. Una modifica della password viene applicata tecnicamente al primo login.  I dipendenti sono istruiti a gestire le password con attenzione e a non renderle accessibili ad altre persone. |
|  | Quali sono i requisiti per la complessità delle password? | Sono accettate solo le password che non fanno parte del login o del nome utente, contengono 3 su 4 classi di caratteri diversi e sono lunghe almeno 8 caratteri. |
|  | Come viene garantito che l'utente possa / debba cambiare regolarmente la sua password? | Le politiche di gruppo (impostazioni di sistema di Microsoft Active Directory) forzano la modifica della password o il blocco dell'accesso dopo 60 giorni. La nuova password non deve corrispondere a una delle tre precedenti. |
|  | Quali precauzioni organizzative vengono adottate per impedire l'accesso non autorizzato ai dati personali sul posto di lavoro? | Le autorizzazioni di accesso sono basate sull'utente e sul gruppo per le persone incaricate dell'elaborazione.  I sistemi sono protetti da password. Le postazioni di lavoro vengono automaticamente bloccate quando non sono attive. I dipendenti sono tenuti a non lasciare dati personali visibili o liberamente accessibili quando lasciano il luogo di lavoro. |
|  | Come si garantisce che le autorizzazioni di accesso siano assegnate in base ai requisiti e per un periodo di tempo limitato? | La direzione controlla regolarmente i diritti e la struttura degli utenti. |
|  | Come vengono documentate le autorizzazioni di accesso? | Tramite le liste di controllo d'accesso nei sistemi. |
|  | Come si garantisce che le autorizzazioni di accesso non vengano utilizzate in modo improprio? | Sporadica revisione dei protocolli di sistema da parte della direzione. |
|  | Per quanto tempo vengono mantenuti i protocolli?  Chi ha accesso ai registri e con quale frequenza vengono valutati? | Nessuna scadenza fissa, di solito i parametri del sistema,  esclusivamente la direzione. |
| **1.4** | **Controllo dell'isolamento** | |
|  | Come si garantisce che i dati raccolti per i diversi scopi siano trattati separatamente? | Un sistema di diritti dedicato viene utilizzato per separare i dati. |
| **1.5** | **Pseudonimizzazione** | |
|  | Quali misure organizzative sono state adottate per garantire che il trattamento dei dati personali sia conforme alla legge? | Formazione regolare sulla protezione dei dati per tutti i dipendenti  Obbligo di tutti i collaboratori alla dichiarazione sulla protezione dei dati |
|  | Come vengono trattati/memorizzati i dati personali in modo che non possano essere ceduti agli interessati? | Nella maggior parte dei casi, il trattamento dei dati personali può essere assegnato a una persona interessata. |
| **2** | **Integrità (articolo 32, paragrafo 1, lettera b) del PILR)** | |
| **2.1** | **Controllo del trasferimento dati** | |
|  | Come garantite l'integrità e la riservatezza nel trasferimento dei dati personali? | La trasmissione dei dati avviene tramite canali cifrati e/o la cifratura dei dati stessi.  I dati di accesso saranno consegnati o comunicati solo al destinatario previsto. |
|  | Per il trasferimento dei dati personali vengono utilizzati sistemi di cifratura e, in caso affermativo, quali? | I dati vengono inviati per e-mail o resi disponibili via Internet tramite server con cifratura di trasporto (TLS).  I dati vengono criptati su un supporto dati utilizzando Microsoft BitLocker e/o archivi ZIP criptati (AES-256). |
|  | Come viene documentato il trasferimento dei dati personali? | n/d |
|  | In che modo la fuga non autorizzata di dati personali viene limitata da misure tecniche? | Una rigorosa attribuzione dei diritti protegge i dati da accessi non autorizzati. |
|  | Esiste un sistema di controllo in grado di rilevare una fuga non autorizzata di dati personali? | Questo viene controllato anche nell'ambito dei controlli di cui al punto 1.3. |
| **2.2.** | **Controllo dell'immissione dei dati** | |
|  | Quali misure vengono adottate per rintracciare chi ha avuto accesso alle applicazioni, quando e per quanto tempo? | Log di accesso ai server e ai sistemi. |
|  | Come si può risalire a quali attività sono state svolte sulle relative applicazioni? | Accedi ai registri delle applicazioni. |
|  | Quali misure vengono adottate per garantire che l'elaborazione da parte dei collaboratori possa essere effettuata solo secondo le istruzioni del cliente? | Formazione e sensibilizzazione dei dipendenti attraverso eventi regolari e colloqui con il personale. |
|  | Quali misure vengono adottate per garantire che anche i subappaltatori eseguano esclusivamente i dati personali del cliente nella misura concordata? | L'elaborazione dei dati dei subappaltatori viene effettuata con una chiara definizione dell'ordine e un ordine formalizzato. |
|  | Come viene garantita la cancellazione/il blocco dei dati personali al termine del periodo di conservazione per i subappaltatori? | In base all'obbligo contrattuale, se lo scopo non è più valido, viene indicata anche la cancellazione dei dati. |
| **3** | **Disponibilità e resilienza (articolo 32, paragrafo 1, lettera b) del PILR)** | |
| **3.1.** | **Controllo della disponibilità** | |
|  | Come si garantisce che i supporti dati siano protetti dagli influssi elementari (fuoco, acqua, radiazioni elettromagnetiche, ecc.)? | I supporti dati di backup sono memorizzati in un'apposita cassaforte.  I record di backup vengono regolarmente esternalizzati dalla direzione. |
|  | Quali misure di protezione vengono utilizzate per la protezione contro il malware e come viene garantita la loro attualità? | Gli aggiornamenti di sicurezza del sistema operativo e i software antivirus e le definizioni vengono distribuiti e aggiornati in modo centralizzato e automatico.  Le soluzioni antivirus e firewall sono utilizzate su sistemi client e server.  Le mail in arrivo vengono controllate dal server di trasporto della posta per verificare la presenza di malware e di dati di invio falsificati prima della consegna. |
|  | Come si garantisce che i supporti dati non più necessari o difettosi vengano smaltiti correttamente? | I supporti dati vengono smaltiti centralmente dal reparto IT.  I supporti dati funzionanti vengono cancellati in modo sicuro secondo metodi adeguati. (ad es. sovrascrittura multipla)  I supporti dati non funzionali sono fisicamente distrutti. |
| **3.2.** | **Recupero rapido** | |
|  | Quali misure organizzative e tecniche vengono adottate per garantire la disponibilità dei dati e dei sistemi il più rapidamente possibile in caso di danno? (recuperabilità rapida secondo l'art. 32 cpv. 1 lett. c GDPR) | I sistemi di server e di alimentazione dell'impianto di elaborazione sono progettati in modo ridondante per evitare un guasto. |
| **4.** | **Procedure per la verifica, la valutazione e l'esame periodico (articolo 32, paragrafo 1, lettera d) del PILR; articolo 25, paragrafo 1 del PILR)** | |
|  | Quali sono le procedure di valutazione/revisione regolare per garantire la sicurezza del trattamento dei dati (gestione della protezione dei dati)? | Il responsabile esterno della protezione dei dati verifica regolarmente e in parte senza preavviso il rispetto delle misure tecnico-organizzative. |
|  | Come reagite alle richieste e ai problemi (Incident-Response-Management)? | Utilizzo di un sistema di biglietteria (kayako) a due livelli (1° e 2° livello); inoltre hotline telefonica e monitoraggio automatico e allarmante |
|  | Quali sono le impostazioni predefinite favorevoli alla protezione dei dati (art. 25 cpv. 2 GDPR)? | Nessuna preassegnazione tramite segni di spunta; non vengono effettuate preassegnazioni al momento dell'accesso al sistema; l'utente deve inserire le informazioni di accesso in ogni caso |
| **4.1** | **Controllo dell'ordine o del contratto** | |
|  | Quali sono le procedure per l'istruzione o la gestione dell'elaborazione dei dati dell'ordine (gestione della protezione dei dati)? | I contratti sono stati redatti in conformità alle nuove linee guida per l'elaborazione dei dati degli ordini. Il responsabile esterno della protezione dei dati svolge i relativi compiti di consulenza e controllo |

**Informazioni legali / Impronta**

Le informazioni contenute in questo documento riflettono lo stato delle conoscenze al momento della creazione del documento. Sono riservati gli errori e le successive modifiche.

estos GmbH declina ogni responsabilità per danni causati dall'uso diretto o indiretto del presente documento. Tutti i marchi e i nomi di prodotti citati sono marchi o proprietà dei rispettivi proprietari.

Copyright estos GmbH. Tutti i diritti riservati.

estos GmbH, Petersbrunner Str. 3a, 82319 Starnberg, Germania

[info@estos.de](mailto:info@estos.de)  
[www.estos.de](http://www.estos.de/)