Accordo di elaborazione dati
allegato 1: **Concetto di protezione dei dati**

Versione: 2.5, 17.08.2023
Referente: Matthias Menne, responsabile della protezione dei dati di onOffice GmbH

Introduzione

l'allegato 1 descrive le misure tecniche e organizzative ai sensi dell'art. 32 del GDPR, volte a garantire la sicurezza dei seguenti trattamenti che sono oggetto del contratto:

- soluzione software CRM online onOffice enterprise
- hosting di siti web
- importazioni di dati
- trasferimenti di dati
- hosting di email

Molti dei trattamenti avvengono sugli stessi sistemi informatici e con le stesse misure di sicurezza. Pertanto, queste misure di sicurezza comuni sono descritte all'inizio di ogni capitolo, per poi concentrarsi sulle singole operazioni.

Crittografia

Il traffico di rete da e verso onOffice enterprise è protetto da https. Sono supportate le versioni TLS 1.0, 1.1 e 1.2. Il certificato è stato rilasciato da "GMO GlobalSign Inc", Portsmouth NH, USA.

I siti web possono essere protetti da certificati verificati dalla CA "Let's Encrypt", San Francisco CA, USA.

I supporti di dati inviati nell'ambito dell'importazione dei dati vengono crittografati prima di essere rinviati ai clienti.

Per l'invio di email viene utilizzato TLS con Perfect Forward Security, a condizione che sia supportato dal server del destinatario.

Riservatezza

La riservatezza dei dati personali viene garantita assicurando che l'accesso fisico o logico ad essi sia riservato esclusivamente a persone autorizzate.

Controllo accessi

Salvo diversa indicazione, tutti i trattamenti avvengono nel centro elaborazione dati di Telehouse Deutschland GmbH (allegato 2).

Qui il controllo degli accessi è garantito da un sistema di badge contactless, dalla presenza di un team di sicurezza 24/7 e dalla videosorveglianza. L'autorizzazione di accesso alle singole sale server è programmata per ogni sala.

I backup vengono memorizzati negli spazi affittati da Telehouse Deutschland GmbH presso il data center di Düsseldorf di Equinix (Germany) GmbH.

I dipendenti dei due centri elaborazione dati non hanno accesso fisico o logico ai dati archiviati.

Nei locali commerciali di onOffice GmbH ad Aquisgrana, i dati personali dei clienti vengono memorizzati solo per un breve lasso di tempo e per i test interni del software (se strettamente necessario) o per l'importazione dei dati. L'assegnazione delle chiavi ai dipendenti è regolamentata e documentata. Al di fuori dell'orario di lavoro, i locali commerciali sono protetti da un sistema di allarme; in caso di allarme, un guardiano di sicurezza viene automaticamente avvisato.

I supporti di dati inviati nell'ambito dell'importazione dei dati sono conservati in totale sicurezza nei locali dell'azienda. Il luogo in cui si trovano i supporti di dati è documentato per iscritto. L'importazione dei dati avviene su un server negli uffici di onOffice GmbH ad Aquisgrana. Il server si trova in una apposita sala server, protetta da un sistema di allarme, registrazione degli accessi e videosorveglianza.

Accesso

È possibile accedere a onOffice enterprise/smart solo inserendo il nome del cliente corretto, il nome di un utente attivo e non bloccato e la password valida. Il nome utente e la password non sono visibili in chiaro quando vengono inseriti. La frequenza di modifica della password può essere configurata nel software stesso da un utente con diritti di amministratore. La complessità di una password viene controllata automaticamente durante l'inserimento di una nuova password; se è al di sotto di un determinato valore, la password non viene accettata.

L'accesso ai sistemi produttivi è limitato al gruppo di persone strettamente necessario ed è protetto dall'autenticazione a crittografia asimmetrica. Gli accessi vengono cancellati ai dipendenti che cessano di lavorare in onOffice.

Il software standard installato sui server viene controllato regolarmente per verificare l'eventuale presenza di aggiornamenti critici per la sicurezza. Questi vengono quindi installati nel più breve tempo possibile senza compromettere la capacità di utilizzo.

I dati personali dei clienti saranno trattati dai dipendenti di onOffice GmbH al di fuori dei locali commerciali solo nella misura necessaria. In questo caso, la politica di sicurezza informatica viene rispettata analogamente a quanto avviene all'interno dei locali aziendali.

Il traffico di rete è monitorato da un firewall hardware.

Accesso ai record di dati

In onOffice enterprise/smart si può l'accesso ai record di dati in modo specifico per ogni utente. A tal fine, i record di dati devono essere collegati a utenti o gruppi specifici e i diritti degli utenti opportunamente limitati. Inoltre, è possibile prenotare un modulo con cui impostare i diritti di visualizzazione e modifica per i singoli record di contatto / immobile / attività per ciascun utente. Gli utenti possono creare un elenco degli ultimi record di dati consultati.

Le caselle di posta elettronica in onOffice enterprise/smart possono essere collegate a uno o più utenti. A questo punto la casella di posta elettronica in questione non sarà più visibile agli altri utenti.

Integrità

Le modifiche apportate ai dati di contatti e immobili in onOffice enterprise/smart vengono tracciate. Gli utenti con diritti di amministratore possono consultare tali modifiche.

onOffice enterprise/smart è in grado di gestire più clienti. I dati di ciascun cliente vengono memorizzati in un database separato. Un utente non può visualizzare i dati di versioni di altri clienti senza aver effettuato l'accesso alla relativa versione specificando il nome del cliente, l'utente e la password.

Le modifiche al codebase di onOffice enterprise/smart vengono accuratamente testate e poi rese disponibili soltanto a un gruppo limitato di clienti per alcune settimane. Solo in seguito saranno estese a tutti i clienti. Le correzioni dei problemi vengono applicate a tutti i clienti due volte alla settimana, in casi urgenti immediatamente.

Gli allegati delle email vengono controllati per verificare la presenza di virus, la protezione antivirus viene applicata agli altri processi.

Disponibilità

Ogni notte viene eseguito un backup completo dei database dei clienti. Questi backup vengono memorizzati negli spazi affittati da Telehouse Deutschland GmbH presso il data center di Düsseldorf di Equinix (Germany) GmbH (vedi Allegato 2). Una volta al mese viene eseguito il backup completo dei file dei clienti e ogni notte il backup incrementale.

Ad eccezione delle "importazioni di dati" e dei "trasferimenti di dati", tutti i trattamenti vengono effettuati nel centro elaborazione dati di Telehouse. La disponibilità dei dati è garantita da un impianto elettrico di emergenza con ridondanza N+1, antincendio con rilevatori ottici / termici e sistemi di estinzione, nonché da connessioni di rete ridondanti a diversi carrier.

In tutti i trattamenti la performance dei computer è sufficiente a compensare il guasto di alcuni server. I dati dei clienti sono archiviati in un sistema RAID 5.

Per proteggersi da attacchi DDoS, onOffice si affida alla rete Prolexic di Akamai. Tutte le richieste ai sistemi di onOffice GmbH vengono gestite tramite i server Akamai. Le richieste che fanno parte di un attacco DDoS vengono filtrate e bloccate.

Liceità del trattamento

Tutti i dipendenti della onOffice GmbH sono tenuti a mantenere la riservatezza dei dati e sono stati formati sul tema della protezione dei dati e della sicurezza informatica.

Sono stati stipulati accordi per l'elaborazione degli ordini con tutti i subappaltatori. Prima della stipula del contratto viene verificata l'idoneità dei subappaltatori. Si garantisce così che anche i dipendenti dei subappaltatori si siano impegnati alla riservatezza.

Il principio di minimizzazione dei dati viene sempre applicato alla progettazione di funzionalità e processi ("Privacy by Design").

Gestione della protezione dei dati

Il concetto di protezione dei dati viene applicato attraverso istruzioni di lavoro, accordi e misure tecnico-organizzative. L'adeguatezza del concetto di protezione dei dati viene verificata almeno una volta all'anno. Se necessario, il concetto di protezione dei dati o la sua applicazione vengono adattati.

Gestione degli incidenti

I sistemi informatici utilizzati per il trattamento sono costantemente monitorati. In caso di incidenti, l'accesso ai dati personali viene ripristinato nel più breve tempo possibile. In seguito agli incidenti, viene effettuato un controllo di follow-up per determinare se è necessario rivedere il concetto di sicurezza informatica o di emergenza informatica e se le misure tecnico-organizzative e l'infrastruttura informatica siano sufficienti a prevenire un incidente dello stesso tipo in futuro.

Trattamento dei dati in paesi terzi

onOffice utilizza la rete Prolexic di Akamai. Per garantire una protezione ottimale contro gli attacchi DDoS, il traffico verso i sistemi di onOffice GmbH viene gestito da server in tutto il mondo. Il traffico è monitorato negli Stati Uniti. Pertanto, i seguenti dati personali possono essere trattati al di fuori dell'UE:

1. indirizzo IP del cliente
2. dominio richiesto
3. URL (per traffico non protetto da https)

onOffice ha stipulato con Akamai le clausole contrattuali standard dell'UE, come emendate a giugno 2021, utilizzando il modulo 3 (da responsabile a responsabile del trattamento).

Sono state effettuate una verifica della situazione legale negli Stati Uniti e un'analisi dei rischi. Il responsabile del trattamento non deve adottare ulteriori misure di sicurezza.