ESEB
Ente Sistema Edilizia Brescia

ACCORDO DI TRATTAMENTO DEI DATI

Autore	Versione documento
Palladini Aldo	1.3

Ente Sistema Edilizia Brescia
via della Garzetta 51
25133 Brescia
tel. 030 2007193
c.f. 80012610178

Ente certificato da
TÜV SÜD Italia
UNI EN ISO 9001-2015
Certificato nr. 501002193

1. OGGETTO

1.1. Oggetto delle presenti condizioni è definire le modalità operative grazie alle quali il Responsabile del trattamento l' **Ente Sistema Edilizia Brescia** (in seguito **E.S.E.B.**) si impegna ad effettuare, per conto del Titolare (***Azienda iscritta al sistema edile)***, le operazioni di trattamento dei dati personali che carica o fornisce in altro modo a **E.S.E.B.** in relazione ai servizi e al trattamento di qualsiasi dato personale che **E.S.E.B.** fornisce al **Cliente** in relazione al servizio.

2. OBBLIGHI DI E.S.E.B.

Le parti, convengono, in relazione alle attività di trattamento dati, quanto segue:

2.1. Che i dati degli interessati oggetto di trattamento saranno processati esclusivamente per le finalità inerenti all'esecuzione del servizio

2.2. Che la tipologia di dati personali e le categorie degli interessati al trattamento si limiteranno esclusivamente a quelli previsti dal servizio

2.3. **E.S.E.B.** dovrà trattare dati personali soltanto su istruzione documentata del titolare del trattamento

3. MISURE TECNICHE ED ORGANIZZATIVE

3.1. **E.S.E.B.** dovrà garantire che le persone autorizzate al trattamento dei dati personali abbiano preventivamente sottoscritto un accordo di riservatezza.

3.2. **E.S.E.B.** dovrà nominare, ai sensi dell'articolo 28, par. 2 del regolamento UE 2016/679 un altro responsabile esclusivamente previa esplicita approvazione da parte del titolare.

3.3. **E.S.E.B.** dovrà mantenere le misure tecniche ed organizzative al fine di assicurare un livello di sicurezza adeguato al rischio.

3.4. Il **Cliente** si riserva il diritto di verificare e monitorare lo stato di conformità del responsabile alle indicazioni fornite in materia di protezione dei dati, anche attraverso audit periodici da parte del proprio personale o di personale esterno incaricato.

4. I DIRITTI E LE RICHIESTE DEGLI INTERESSATI

4.1. **E.S.E.B.** dovrà assistere il titolare del trattamento avvalendosi di misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato ai sensi dell'articolo 15 del regolamento UE 2016/679.

4.2. Nell'eventualità che a **E.S.E.B.** vengano avanzate richieste da parte degli interessati circa l'esercizio dei propri diritti inerenti ai dati personali di proprietà del **Cliente**, a titolo esemplificativo e non esaustivo rettifica, cancellazione e limitazione, portabilità dei dati, **E.S.E.B.** dovrà informare il **Cliente**, senza ritardo e comunque non oltre i termini di legge.

4.3. Nell'eventualità che il Titolare sia obbligato a fornire informazioni su dati personali ad altri titolari o terzi, **E.S.E.B.** ha l'obbligo di collaborare fornendo tutte le necessarie informazioni.

5. COMUNICAZIONI DEI DATI A TERZI

5.1. **E.S.E.B.** potrebbe divulgare i dati a terzi, alla pubblica amministrazione o all'Autorità giudiziaria, senza la preventiva autorizzazione del Titolare dei Dati Personali, sempre nel rispetto delle finalità perseguite dell'Ente Paritetico e stabilite dal Contratto Collettivo Nazionale e dagli Accordi Collettivi territoriali. Nell'eventualità che la comunicazione di dati e l'accesso ad essi siano richiesti dal diritto dell'Unione Europea o dal Diritto Nazionale, **E.S.E.B.** dovrà comunicare i dati al richiedente e, successivamente, notificare tale avvenimento al titolare del trattamento, comunicando altresì tale obbligo giuridico; tutto quanto precedentemente spiegato, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

6. RESTITUZIONE O CANCELLAZIONE DEI DATI PERSONALI

6.1. Salvo diverse disposizioni di legge, **E.S.E.B.**, a seconda della scelta del Titolare del trattamento dei Dati Personali, dovrà cancellare o restituire i dati personali al termine o alla cessazione dell'accordo; si impegna inoltre, a cancellare le copie esistenti, su richiesta del titolare del trattamento, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati oltre il limite stabilito dal titolare.

7. ASSISTENZA E REGISTRI

7.1. **E.S.E.B.** dovrà mantenere e di volta in volta aggiornare il registro contenente i nomi e dettagli di contatto dei subfornitori.

7.2. **E.S.E.B.** dovrà mantenere un registro degli accessi ai dati personali da parte di una pubblica amministrazione, autorità giudiziaria o audit di terze parti.

7.3. **E.S.E.B.** dovrà mantenere un registro delle violazioni che coinvolgano i dati personali degli interessati.

7.4. Altresì, **E.S.E.B.** compilare il registro delle attività di trattamento, ai sensi dell'art.24 avendo cura di comunicare al titolare del trattamento le categorie di attività di trattamento svolte per conto dello stesso e gli eventuali subfornitori coinvolti.

8. TRASFERIMENTO DEI DATI EXTRA UE

8.1.Nome Fornitore potrà fornire al Titolare ulteriori informazioni e documenti relativi al meccanismo per il trasferimento internazionale dei dati ai sensi dell'articolo 46 del GDPR.

8.2.Nell'eventualità in cui Nome Fornitore trasferisca i dati ad un subfornitore di Nome Fornitore che ha sede negli Stati Uniti d'America dovrà comunicare al Titolare informazioni sulla certificazione al programma di Privacy Shield del subfornitore di Nome Fornitore e regolarmente, almeno annualmente, confermare che la certificazione al programma di Privacy Shield del Subfornitore di Nome Fornitore sia valida.

9. SUBFORNITORI DI E.S.E.B.

9.1. Il titolare dei Dati Personali, a mezzo di posta elettronica certificata, ove possibile, altrimenti mediante email, dovrà approvare la lista dei subfornitori ed i contratti stipulati con essi. Il responsabile, inoltre, dovrà notificare mediante gli strumenti succitati, preventivamente e senza alcun ritardo al titolare, eventuali variazioni rispetto alla lista di subfornitori precedentemente accordata.

9.2. **E.S.E.B.** deve far rispettare ai subfornitori approvati le obbligazioni assunte in questa DPA.

9.3. Nel caso in cui il responsabile, ai sensi dell'articolo 28, par. 4 del Regolamento UE 2016/679, nomini un subfornitore, a quest'ultimo sono imposti gli stessi obblighi vigenti tra titolare e **E.S.E.B.**.

9.4. Qualora il subfornitore ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento del subfornitore.

10. VIOLAZIONE DEI DATI PERSONALI

9.1 **E.S.E.B.** ha l'obbligo di informare senza ritardo (entro 24 ore dalla nascita del sospetto) ogni sospetto di non conformità al Regolamento Europeo 2016/679 o a i termini contrattuali presenti in questa DPA o in caso di gravi problemi alle operazioni di trattamento dei dati o ogni altra irregolarità nel trattamento dei dati personali di proprietà del **Cliente**. **E.S.E.B.** dovrà prontamente verificare e rettificare ogni non conformità e su richiesta del **Cliente** fornire tutte le informazioni e chiarimenti desiderati circa il sospetto di non conformità.

9.2 Nell'eventualità di violazioni, **E.S.E.B.** dovrà comunicarlo al Titolare del trattamento dei dati, senza ritardo e comunque entro e non oltre 24 ore. **E.S.E.B.** dovrà prontamente verificare le modalità di violazione dei dati e fornire al Titolare del trattamento dei dati tutta l'assistenza necessaria ad adempiere a tutti gli obblighi di legge (incluso il dover comunicare l'evento all'Autorità Garante e all'interessato).

9.3 Per chiarezza, **E.S.E.B.** dovrà notificare al Titolare del Trattamento dei dati in primis, qualsiasi incidente di sicurezza che coinvolga i dati personali degli interessati ed in secondo luogo, quegli incidenti accaduti ai subfornitori nominati dal responsabile entro e non oltre le 24 ore dal momento del rilevamento dell'incidente.

10. DURATA

10.1. Il presente accordo è valido fino alla cessazione dei Servizi. **E.S.E.B.** dovrà mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

10.2. **E.S.E.B.**, all'atto della scadenza dei Servizi, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta del Titolare, all'immediata restituzione allo stesso dei Dati Personali oppure alla loro integrale cancellazione, in entrambi i casi

rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia. In caso di richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

11. GIURISDIZIONE E MEDIAZIONE

11.1. Controversie, domande e contenziosi tra le parti, concernenti questo accordo devono essere instauranti avanti il Foro di Brescia

11.2. Il presente Accordo è regolato dalla legge italiana.

Allegato 1 - Misure di sicurezza -

E.S.E.B. manterrà tutte le appropriate misure tecniche ed organizzative di sicurezza in conformità con i Principi di Sicurezza dei Dati del GDPR, al fine di proteggere i dati di proprietà del Cliente da fughe accidentali, distruzione, alterazione, accessi o rivelazioni non autorizzate.

OPZIONE A – ATTESTAZIONE INDIPENDENTE DI SICUREZZA

Il fornitore ha implementato e mantiene un SGSI conforme alle previsioni di una o più delle seguenti norme:

- ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems – Requirements.
- ISO/IEC 27018:2014 - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (se applicabile)
- Service Organization Control (SOC) 2 Tipo II.

Il fornitore deve essere munito di una attestazione in corso di validità.

Annualmente, il fornitore dovrà provvedere ad aggiornare e mantenere le proprie certificazioni; dovrà, inoltre, mostrare la durata di validità dell'attestazione.

Il fornitore dovrà fornire a COMPANY NAME una copia della propria certificazione entro e non oltre 30 giorni dal ricevimento della stessa o su richiesta di COMPANY NAME.

OPZIONE B – GDPR PRINCIPI DI SICUREZZA DEI DATI

Nell'ambito delle attività di trattamento oggetto del presente contratto, il titolare del trattamento dispone che il responsabile osservi le seguenti misure di sicurezza durante lo svolgimento di attività di trattamento:

1. Conservare i dati degli interessati all'interno di archivi protetti se necessario cifrati, siano essi contenuti in dispositivi mobili sia in dispositivi di storage condivisi. In caso di cifratura si raccomanda di scegliere una chiave crittografica sicura e adeguata alla natura dei dati personali coinvolti.

2. Limitare la diffusione dei dati personali degli interessati alle sole parti autorizzate.

3. Permettere l'accesso ai dati personali da parte degli utenti secondo la regola del "minimo privilegio"

4. Utilizzo di adeguato sistema di autenticazione degli utenti ai sistemi che trattano dati personali

5. Registrare e monitorare l'accesso da parte degli utenti dei sistemi ai dati personali in modo da garantire una catena di responsabilità chiara e verificabile.

6. Conservare i log di accesso rilevanti (anomalie) ai sistemi e ai dati personali per tutta la durata dell'attività di trattamento.

7. Registrare tutti gli accessi ai log dei sistemi da parte degli utenti dotati di diritti amministrativi.

8. Vietare l'utilizzo di utenze condivise tra gli utenti per l'accesso ai sistemi e ai dati.

9. Segregare a livello logico il network, in modo tale che gli utenti "Guest" non possano accedere alla stessa sottorete degli utenti dei sistemi dell'azienda. In generale, laddove possibile utilizzare più sottoreti logiche (VLAN) ognuna dotata di specifiche regole (ACL) per l'accesso ai servizi e le risorse di rete.

10. Utilizzare il protocollo di sicurezza adeguati per le reti Wi-Fi

11. Segregare fisicamente il network, in modo tale che solo il personale autorizzato possa accedere agli apparati di rete.

12. Utilizzare esclusivamente protocolli di comunicazione sicuri come TLS 1.2 E SSH per le sessioni di comunicazioni client-server.

13. Permettere l'accesso remoto alle risorse informatiche solo ed esclusivamente attraverso canali sicuri che rendano il traffico dati non intercettabile (es: IPsec, etc)

14. Custodire in appositi “contenitori” le chiavi crittografiche utilizzate sia per gli applicativi che per le comunicazioni.

15. Inibire l’accesso da parte degli utenti dei sistemi al network TOR (The Onion Routing).

16. Utilizzare esclusivamente sistemi di storage mobili (USB) dotati di adeguata protezione crittografica nel trasporto di dati personali degli interessati.

17. Dotarsi di soluzioni di MDM/MDA qualora gli utenti utilizzino o conservino dati personali degli interessati su dispositivi mobili, siano essi di proprietà aziendale (COPE) sia in modalità promiscua (BYOD)

18. Utilizzare il protocollo SFTP per il trasferimento massivo dei dati, proibire l’uso del FTP.

19. Inibire l’utilizzo da parte degli utenti di sistemi personali di private cloud (es: DropBox, Gdrive, wetransfer etc) per la conservazione e il trasferimento di file contenenti dati personali degli interessati.

20. Utilizzare esclusivamente sistemi di istant-messagging che prevedano l’utilizzo di protocolli OTR (Off the record)

21. Utilizzare i protocolli PGP o S/MIME per la protezione crittografica del contenuto delle mail

22. Dotarsi di adeguati sistemi in grado di garantire la continuità del servizio erogato (business continuity) per conto del titolare, tale per cui, in caso di incidente di sicurezza lo stesso non comprometta la disponibilità dei dati e del servizio erogato per conto o in favore del titolare.

23. Dotarsi di idonea procedura di gestione degli incidenti tale per cui ogni incidente di sicurezza sia individuato, registrato e sia processato da personale specializzato nella sua risoluzione. Ogni incidente dovrà essere, registrato all’interno del registro degli incidenti del responsabile ed in seguito comunicato al titolare del trattamento.