Dataskydd och datasäkerhet

hos COSMO CONSULT-Group som är gemensamt personuppgiftsansvarig, i enlighet med artikel 26 GDPR

Version: 3.2 | Datum: 14.03.2023

Skapad av: Michael Makowski

COSMO CONSULT SSC GmbH
Von Steuben Straße 10 | 12
48143 Münster
Tyskland

dataprotection@cosmoconsult.com
www.cosmoconsult.com

Innehållsförteckning

1 Datasäkerhetsåtgärder på COSMO CONSULT

Detta dokument beskriver de tekniska och organisatoriska åtgärder som vidtagits vid COSMO CONSULT för att säkerställa implementering i enlighet med artikel 32 GDPR:

1.1. COSMO CONSULT har vidtagit åtgärder för att skydda uppgifter och data, samt att driften vid anläggningen inte avbryts, med avseende på konstruktion, personal, organisation och teknik.

1.2. COSMO CONSULT är bundet av sekretess gentemot sina kunder. Alla anställda på COSMO CONSULT förbinder sig att iaktta tystnadsplikt i samband med att de anställs.

1.3. På COSMO CONSULT omfattar detta skydd all hantering av uppgifter om fysiska eller juridiska personer samt andra konfidentiella eller känsliga uppgifter (t.ex. företagsuppgifter eller finansiella uppgifter).

1.4. Brandskyddsåtgärder och olycksförebyggande åtgärder har vidtagits på alla kontor och anläggningar som tillhör COSMO CONSULT.

1.5. In- och utträde kontrolleras vid alla anläggningar genom strukturella säkerhetsåtgärder och i regel elektroniskt övervakade säkerhetsområden. Bortskaffande av konfidentiella dokument utförs uteslutande via dokumentförstörare.

1.6. COSMO CONSULT använder den senaste tekniken från Microsoft, vilken uppfyller alla dataskyddskrav. Detta framgår av olika dataskyddssigill från Microsoft.

1.7. COSMO CONSULT anställer flera IT-specialister (certifierade, vanligtvis genom Microsoft) för att kontrollera säkerhetsåtgärderna, komplettera dem enligt kraven och vidareutveckla dem med hänsyn till de senaste tekniska framstegen.

1.8. COSMO behandlar data under programvaruimplementering, för datamigrering och testning. COSMO CONSULT sätter också upp testsystem i samordning med kunden. Testsystem kommer att finnas kvar så länge support tillhandahålls av COSMO CONSULT eller vad som har överenskommits i avtal. Efter samråd med kunden kan testsystemens dataset vara en datauppsättning som har justerats för känsliga data och simuleras för teständamål. COSMO CONSULT rekommenderar test- och utvecklingssystem körs på servrar eller i kundens molnmiljö.

1.9. I samband med fjärrunderhåll/åtkomst till kundens system finns det alltid ett säkerhetssystem (krypteringsåtgärder etc.) som skyddar mot obehörig åtkomst.

1.10. För att skydda mot datavirus skannas alla inkommande media, e-postmeddelanden och bilagor efter virus. Dessutom skyddas alla datorer och servrar av centralt hanterat ändpunktsskydd.

1.11. COSMO har flyttat nästan alla centrala tjänster och dataskyddskrav till ett centralt datacenter.

1.12. Databehandlingen utförs uteslutande i enlighet med GDPR.

1.13. Om ett avtal om orderbehandling har tecknats med en kund gäller följande ytterligare dataskyddsåtgärder:

1.13.1.1. principen om åtskillnad mellan funktioner tillämpas inom alla viktiga områden. De områden som berörs av databehandling skiljs från varandra funktionellt och organisatoriskt. Kundsystem är endast tillgängliga för behöriga personer, respektive projekt- eller kundteam. Åtkomsträttigheterna tilldelas av ansvarig projektledare och kontrolleras regelbundet.

1.13.2. Anslutningsdata som behövs för fjärrunderhåll är antingen personliga eller begränsas till behöriga anställda i respektive projekt eller kundteam, beroende på kundens krav.

1.14. Dataskydd och datasäkerhet är av största vikt för COSMO CONSULT och företaget granskar därför sina interna processer regelbundet.

2 Dataskyddsåtgärder vid COSMO CONSULT

2.1. De tekniska och organisatoriska dataskyddsåtgärderna (TOM) är följande:

2.1.1. Orderkontroll, fysisk åtkomstkontroll, logisk åtkomstkontroll, behörighetskontroll, överföringskontroll, indatakontroll, tillgänglighetskontroll, kontroll av åtskillnad och effektivitetskontroll.

2.1.2. Typ av datautbyte, tillhandahållande av data, typ och villkor för behandling, datalagring samt typ och villkor för dataöverföring

2.1.3. Åtgärder för att hela tiden säkerställa konfidentialitet, integritet, tillgänglighet och robusthet för system och tjänster, samt möjligheten att snabbt återställa åtkomsten och tillgängligheten till personuppgifter i händelse av en fysisk eller teknisk incident.

2.1.4. Ett förfarande för regelbunden översyn, utvärdering och validering av dessa åtgärders effektivitet.

2.2. I den mån enskilda värdtjänster av leverantörer kommer COSMO CONSULT att noggrant välja dessa i enlighet med rättsliga kraven, teckna skriftliga avtal och informera kunderna om uppgiftsbehandlingen i det avtal som skall ingås.

2.3. COSMO CONSULT Group kontrollerar och övervakar löpande att de tekniska och organisatoriska åtgärderna som införts av samtliga företag som ingått ett avtal om gemensamt personuppgiftsansvar i enlighet med artikel 26 GDPR.

2.4. De tekniska och organisatoriska åtgärderna på COSMO CONSULT grundas i allmänhet på tekniska framsteg och vidareutveckling. COSMO CONSULT kommer att vidta alla nödvändiga åtgärder för att öka säkerheten.

Den senaste dokumentationen av de tekniska och organisatoriska åtgärderna "dataskydd och datasäkerhet hos COSMO CONSULT" finns tillgänglig för nedladdning på webbplatsen https://www.cosmoconsult.com/data-protection.

3 Platser för databehandling

3.1 COSMO CONSULTS centrala datacenter

COSMO CONSULT använder Microsoft Azure för alla centrala tjänster och servrar.

Se även https://azure.microsoft.com.

3.2 Anläggningar hos COSMO CONSULT

COSMO CONSULT är en internationell företagsgrupp med flera anläggningar som genomför IT-projekt över hela världen. De åtagande och åtgärder som angetts här gäller för alla anläggningar som tillhör COSMO CONSULT Group.

Se https://www.cosmoconsult.com/data-protection

3.3 Databehandling i Microsoft Azure

COSMO CONSULT driver sina molnbaserade tjänster och servrar i Microsoft Azure-plattformen. Västeuropa (Amsterdam, Nederländerna) har valts ut som huvudplats för databehandling, med enskilda tjänster som finns på andra europeiska platser.

I den mån data lagras på Azure-plattformen inom ramen för kundorder och det sker en överföring av personuppgifter till ett tredjeland inom Microsoft Azure-molnet, har COSMO CONSULT ingått ett avtal med Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Irland, i enlighet med de rättsliga kraven på grundval av EU:s standardavtalsklausuler och har kontrollerat de ytterligare skyddsåtgärder som vidtagits av Microsoft.

4 Tekniska och organisatoriska åtgärder

4.1 Sekretess (Art. 32 1b GDPR)

4.1.1 Fysisk åtkomstkontroll

Nedan listas de åtgärder som förhindrar forcerat eller obehörigt intrång i lokaler som tillhör COSMO CONSULT.

- besöksregistrering i receptionen
- lokala serverrum (om tillämpligt) är dessutom säkrade på alla platser i kontorsbyggnaderna.
- personlig/kontrollerad ledsagning av besökare
- låssystem
- nyckelregler och nyckelbok (användning av säkerhetsnycklar)

4.1.2 Logisk åtkomstkontroll

COSMO CONSULT säkrar användningen av databehandlingssystemen genom olika åtkomstkontroller, så att endast behöriga personer har tillgång till dem. Varje åtkomst kräver identifiering och autentisering av användaren. Åtkomst utifrån är säkrad av en brandvägg på alla platser.

- autentisering med användarnamn och lösenord
- användarprofiler
- användning av programvara för ändpunktsskydd
- användning av brandväggar
- användning av VPN-teknik
- regler för tilldelning och ändring av lösenord
- obligatoriskt med automatiskt skärmlås (lokalt)
- nyckelregler och nyckelbok (användning av säkerhetsnycklar)
- kryptering av externa/mobila enheter
- kryptering av interna datamedier
- hanterade användare och användarbehörigheter

4.1.3 Kontroll av dataåtkomst

Nedan listas COSMO CONSULTS åtgärder som garanterar att de med behörighet att använda ett databehandlingssystem endast kan få tillgång till de uppgifter de tillhandahållit, och att personuppgifter inte kan läsas, kopieras, ändras eller raderas utan tillstånd under behandling, användning och efter lagring.

- auktoriseringskoncept (AD-grupper, rolldefinitioner)
- användning av dokumentförstörare eller insamlingsbehållare (system för bortskaffande av dokument)
- lösenordspolicy
- systemadministratörer administrerar användarrättigheter

4.1.4 Kontroll av åtskillnad

Nedan listas COSMO CONSULTS åtgärder för att säkerställa att uppgifter som samlats in för olika ändamål kan behandlas separat.

- åtskilda databaser och multitenants
- definition av behörigheter för olika kunder
- åtskilda produktions- och testsystem

4.2 Integritet (Art. 32 1b GDPR)

4.2.1 Kontroll av dataöverföring

Nedan listas COSMO CONSULTS åtgärder för att säkerställa att personuppgifter inte kan läsas, kopieras, ändras eller raderas utan godkännande under elektronisk

överföring eller i samband med transport eller lagring hos databärare, och att de kan verifieras och fastställas var personuppgifter kommer att överföras.

- regler för användning av externa/mobila enheter
- noggrann rekrytering av medarbetare
- VPN-tunnel till COSMO CONSULT-nätverket

Beskrivning av de åtgärder som ska vidtas av den registeransvarige:

- loggning av dataöverföringar
- VPN-tunnel till kundens nätverk

4.2.2 Indatakontroll

Nedan listas COSMO CONSULT:s åtgärder för att säkerställa att det vid ett senare tillfälle kan verifieras och fastställas om och av vem personuppgifter har matats in, ändrats eller raderats i databehandlingssystem.

De tekniska och organisatoriska åtgärderna med avseende på indatakontroll måste vidtas på kundens sida.
Det är kundens ansvar att tilldela enskilda användarnamn i stället för kollektiva inloggningar för personalgrupper eller team (från COSMO CONSULT för att stödja kunden). Det är också kundens ansvar att logga transaktioner så det går att spåra inmatning, ändring och radering av data i produktionssystemet.

- loggning av inmatning, ändring och radering av uppgifter genom enskilda användarnamn (inte användargrupper)
- loggning av inmatning, ändring och radering av data (ändringslogg eller liknande)
- tilldelning av rättigheter för att mata in, ändra och radera data baserat på ett behörighetskoncept

4.3 Tillgänglighet och återställande (Art. 32 1b GDPR)

4.3.1 Tillgänglighetskontroll

Nedan listas COSMO CONSULT:s åtgärder för att säkerställa att personuppgifter skyddas mot oavsiktlig skada eller förlust, och att se till att de skyndsamt kan återställas i händelse av en incident.

De tekniska och organisatoriska åtgärderna med avseende på tillgänglighetskontroll måste vidtas från hos kunden.

De tekniska och organisatoriska åtgärder som vidtas av COSMO CONSULT tjänar uteslutande för interna/egna syften hos COSMO CONSULT och garanterar funktionsduglighet och tillgänglighet.

- hålla säkerhetskopior på en säker plats
- brandsläckare i lokala serverrum (eller i erforderlig närhet)
- försiktighetsåtgärder för säkerhetskopiering och återställning

4.4 Förfaranden för periodisk översyn, bedömning och utvärdering (Art. 32 1d GDPR och Art. 25 1 GDPR)

4.4.1 Orderkontroll

Nedan listas COSMO CONSULTS åtgärder som säkerställer att personuppgifter som behandlas av andra leverantörer på uppdrag av COSMO CONSULT endast kan behandlas i enlighet med kundens instruktioner.

En förteckning över godkända underleverantörer uppdateras regelbundet på https//www.cosmoconsult.com/data-protection. Vid ändringar kommer kunderna att informeras i förväg via e-post.

- val av leverantör med avseende på tillbörlig aktsamhet (särskilt när det gäller datasäkerhet)
- avtal avseende typ och omfattning, samt syfte med den personuppgiftsansvariges beställning och användning av personuppgifter
- endast skriftliga avtal om orderbehandling
- endast skriftliga instruktioner till underleverantören
- skyldighet för underleverantörens anställda att upprätthålla datasekretess

4.4.2 Organisatorisk kontroll

Nedan listas COSMO CONSULTS åtgärder som säkerställer att den interna organisationen uppfyller de särskilda kraven på dataskydd.

- iakttagande av standardinställningar som är anpassade för dataskydd (Art. 25 paragraf 2 GDPR)
- hantering av dataskydd
- deltagande av den globala dataskyddssamordnaren och det externa dataskyddsombudet om de operativa processerna kräver detta
- organisationshandbok på webbplatsen

- regelbundna revisioner för att säkerställa efterlevnad av de tekniska och organisatoriska åtgärderna
- regelbundna vidareutbildningar
- standarder och anvisningar för IT-säkerhet
- standarder och anvisningar för att säkra datamängden

5 Kontakt

5.1 Global integritetssamordnare

COSMO CONSULT SSC GmbH

Mikael Makowski

Von-Steuben-Straße 10/12

48143 Münster

Tyskland

E-postadress: dataprotection@cosmoconsult.com

webb: https://www.cosmoconsult.com

5.2 Externt dataskyddsombud

2b Rådgivning GmbH

Joseph-Schumpeter-Allee 25

53227 Bonn

Tyskland

E-postadress: cosmoconsult@2b-advice.com

webb: https://www.2b-advice.com