Informationssäkerhetsstrategi

Aktiebolaget CoreCode International
version 2.0, juni 2018

Aktiebolaget CoreCode International (nedan kallat CCI) har en huvudsaklig verksamhet i att förse verksamheter och organisationer med tillgång till utbildningar, där vissa personuppgifter behandlas. Detta ställer högra krav på oss som leverantör kring både teknisk och organisatorisk informationssäkerhet.

De övergripande målen för CCI informationssäkerhet är att skapa en juridiskt, driftsmässigt och kundvänlig trygghet kring personuppgifter, i enlighet med Dataskyddsförordningen (GDPR).

Vi ska ha en proaktivt förhållningssätt samt ett professionell ramverk för hur vår informationssäkerhet hanteras. Vår ambitionsnivå ska vara hög kring detta, eftersom det är affärskritiskt för verksamheten.

Personuppgifter behandlas till absolut största del i vår bokningsplattform och vårt CRM. Men personuppgifter skall även behandlas korrekt i annan del av verksamheten, såsom kundkommunikation, supportärenden samt administration.

Detta skall ske genom tydliga policys och rutiner för:
• Övergripande hög prioritering av informationssäkerhet
• Hantering av Personuppgiftsbiträdesavtal
• Val av underleverantörer
• Inbyggt dataskydd
• Behörig personal
• Information till registrerade
• Säkerställande av otvetydligt samtycke
• Administrativ hantering av personuppgifter
• Löpande gallring
• Begäran om dataportabillitet
• Rätten att bli bortglömd
• Effektiv incidenthantering
• Informationssäkerhetsmedvetenhet
• Årlig revision av informationssäkerhetsplanen

Informationssäkerhetsplan

Policys & rutiner

Aktiebolaget CoreCode International
version 2.0, juni 2018

Denna plan beskriver hur CCI arbetar med att hålla en hög informationssäkerhet, både i Plattformen och i övrig verksamhet.

Övergripande hög prioritering av informationssäkerhet
Eftersom informationssäkerhet är affärskritiskt för CCI skall det vara en högt prioriterad fråga i val av rutiner, underleverantörer, förhållningssätt och datahantering.

Rutiner för detta:
I varje val av rutiner, underleverantörer, förhållningssätt och datahantering skall informationssäkerheten finnas som en viktig del av beslutsunderlaget. I varje val skall frågan uppmärksammas så att det inte sker några misstag, där informationssäkerheten sänks.

Val av underleverantörer
Vår absolut viktigaste underleverantör är den som står för utveckling, drift och informationssäkerhet kring vårt bokningssystem och CRM. Men även i val av andra underleverantörer skall vi ha ett högt informationssäkerhetsfokus.

Rutiner för detta:
I fråga om utveckling och drift av våra system skall en svensk underleverantör, med gott renommé och som garantera en svensk, informationssäker driftsmiljö väljas. Denne skall ha mycket god kännedom och kompetens kring informationssäkerhet, för att kunna säkerställa denna.
• I val av andra leverantörer, för exempelvis lagring av dokument eller annan datahantering, skall väl etablerade, i första hand svenska, leverantörer väljas.

Inbyggt dataskydd
I våra system skall alla personuppgifter finnas i en säker datamiljö. Bokningssystem och CRM ska driftas på en svensk server, i ett låst serverrum, dit endast ett fåtal behöriga tekniker har tillträde.
Vi ska regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.
Detta kommer att ske på följande sätt
- En årlig dokumenterad säkerhetskontroll, på lämplig nivå i enlighet med branschstandard.
Övrig lagring av eventuella personuppgifter ska ske på säkert sätt.

Rutiner för detta:
• Tillse att Plattformsleverantören har de organisatoriska och tekniska stöd som krävs.
• Tillse att Plattformsleverantören genomför löpande, dokumenterade säkerhetskontroller.
• Om en kund vill genomföra en tredjeparts säkerhetskontroll av plattformen får denne gärna göra det. Vi bistår i detta, genom att, mot självkostnad, tillhandahålla den information som kan vara relevant i ett sådant sammanhang.

Behörig personal
All hantering av personuppgifter skall bara kunna ske av behörig personal.
Rutiner för detta:
• Endaste ett fåtal personer skall ha tillgång till behörighet till hela bokningssystemet i syfte att kunna hantera bokning och supportärenden. Dessa ska behandla alla uppgifter med varsamhet.

• Alla som hanterar personuppgiftsfrågor på CCI skall vara medvetna om den sekretess som råder kring kund- och användaruppgifter.

Information till registrerade
Det ska vara lätt för en deltagare att få information kring hur Personuppgifter hanteras.

Rutiner för detta:
• Det ska finnas lätt tillgänglig information i systemet, på valt språk, som tydligt beskriver hur personuppgifter hanteras, en Integritetspolicy.
• Informationen skall uppdateras så snart som möjligt efter att ändringar sker.

Säkerställande av otvetydigt samtycke
För att säkerställa otvetydigt samtycke kommer varje deltagare att, i samband med sin första bokning, ge sitt samtycke till behandling av deras personuppgifter, på det språk som valts för användaren. Detta samtycke kommer att loggas och lagras.
Varje användare som har givit samtycke kan via CCI upphäva det, med omedelbar verkan.

Rutiner för detta:
• Tillse att systemadm har de organisatoriska och tekniska stöd som krävs.

Administrativ hantering av personuppgifter
De personuppgifter som hanteras i dokument utanför bokningssystem och CRM skall vara lätta att hitta för att också kunna hanteras.
Rutiner för detta:
• Dokument som innehåller personuppgifter ska märkas och lagras i mappar som tydligt anger kund och uppdrag.
• E-postmeddelanden som innehåller personuppgifter ska hanteras med varsamhet och sändes inte vidare till annan än den som är personsuppgiftsbiträde.

Gallring
Vi åtar oss under löpande avtal efter begäran gallra avaktiverad deltagare.
Gallringen innebär borttagning av alla personuppgifter, med undantag av statistikunderlag, som anonymiseras.

Rutiner för detta:
• För Bokningssystemet: Tillse att leverantören och vår administratör har de organisatoriska och tekniska stöd som krävs, samt följer dessa.
• För administrativa dokument och e-post: Dokument och e-post som innehåller personuppgifter som blivit inaktuella skall raderas senast 12 månader efter att kundrelationen upphört.

Begäran om dataportabillitet
Vi ska bistå personuppgiftsansvarig med individuell begäran om att få personuppgifter utlämnade inom 72 timmar.

Rutiner för detta:
• Tillse att systemleverantören och vår administratör har de organisatoriska och tekniska stöd som krävs.
• Utan dröjsmål bistå berörd Personuppgiftsansvarig, direkt eller via den huvudkontaktperson som finns hos den berörda kunden. Detta gäller även dokument och epostmeddelanden som innehåller personuppgifter om den aktuella personen.

Rätten att bli bortglömd
Vi ska bistå personuppgiftsansvarig med individuell begäran om att bli bortglömd inom 72 timmar.

Rutiner för detta:
• Tillse att systemleverantören och vår administratör har de organisatoriska och tekniska stöd som krävs.
• Utan dröjsmål bistå berörd Personuppgiftsansvarig, direkt eller via den huvudkontaktperson som finns hos den berörda kunden. Detta gäller även dokument och epostmeddelanden som innehåller personuppgifter om den aktuella personen.

Effektiv incidenthantering
Vi ska rapportera incidenter, som dataintrång, kring personuppgifter inom 72 timmar.

Rutiner för detta:
• Tillse att systemleverantören och vår administratör har de organisatoriska och tekniska stöd som krävs.
• Utan dröjsmål rapportera incident till berörd Personuppgiftsansvarig, via den huvudkontaktperson som finns hos den berörda kunden.
• Personuppgiftsansvarige dokumenterar alla personuppgiftsincidenter, omständigheterna kring incidenten, dess effekt samt de korrigerande åtgärder som vidtagits.

Informationssäkerhetsmedvetenhet
Alla som jobbar i CCI verksamhet skall ha god kännedom kring vikten av en hög informationssäkerhet, samt de rutiner som beskrivs här.

Rutiner för detta:
• Varje ny medarbetare/partner ska få en genomgång av vår informationssäkerhetsstrategi och plan.

Årlig revision av informationssäkerhetsplanen
Dessa policys och rutiner skall årligen uppdateras.

Rutiner för detta:
• Vid första tisdagen i februari skall detta dokument gås igenom och revideras vid behov.

Dataskyddsombud
CCI har ett gemensamt dataskyddsombud.
För närvarande är det Helene Palmgren, Kontaktuppgifter: helene.palmgren@corecode.se, +46 76 172 91 51.