Datum: 2018-05-09

Reviderad:

Styrdokument för informationshantering - GDPR

Version 1.0

Evado, Varvsgatan 53, SE-972 33 LULEÅ, SWEDEN
Tel: +46 920 256900 info@evado.se www.evado.se

Innehållsförteckning

1 Inledning

Detta styrdokument beskriver hur vi arbetar med information. För att få ett kontinuerligt arbete med systematisk uppföljning har vi valt att slå ihop rutiner och målbild för filhantering, GDPR och annan informationshantering till ett dokument. Vilket gör att vi säkerställer kvalitén, får in arbetssättet i det vardagliga arbetet och skapar ordning och reda.

1.1 Mål

- Vi hanterar information inom företaget på ett säkert och dynamiskt sätt. Vi följer GDPR, och nya direktiv som kommer för att uppdaterar rutiner och dokument kontinuerligt.
- Vi har en transparant miljö i företaget där vi genom att dela information inom företaget höjer vår kompetens, säkerställer att informationen är korrekt och hålls uppdaterat.
- Vi tillhandahåller rätt verktyg till personal för att de ska kunna hantera information enligt direktiv och känna att de underlättar deras arbete.
- Vi har koll på nya verktyg och system som kan underlätta och effektivisera vårt arbete.
- Vi har en tydlig rutin för att skapa effektivitet, säkerhet och säkerställa god ordning.

1.2 Ansvariga

VD	Rickard Hellgren
Affärsutveckling	Håkan Olsson
Säljansvarig	Jan Vikberg
Marknadsansvarig	Emil Lilja
Leveransansvarig	Albin Nilsson
Förvaltningsansvarig	Albin Nilsson
Produktutvecklingsansvarig	Fredrik Tano
Dataskyddsombud ”teknik”	Fredrik Tano
Dataskyddsombud ”dokumentering”	Rickard Hellgren
Systemadministratörer	Fredrik Tano, Fredrik Hällgren, Albin Nilsson
Projekt	Projektledare

1.3 Klassning av information

Klassning av information kommer följa modellen KLASSA som delas in i nivåerna:

0. Ingen eller försumbar skada
1. Måttlig skada
2. Betydande skada
3. Allvarlig skada
4. Synnerligen allvarlig skada

Mer information om modellen finns: https://klassa-info.skl.se/demo/impactassesment
Klassningen delas in i Konfidentialitet, Riktighet och Tillgänglighet.

Konfidentialitet (Säkerhet), bedöms på varje dokument, projekt eller information som skapas. Bedömning av konfidentialitet skrivs in i beskrivning, anteckning eller dokument direkt via dokumentmallen.

0. Öppen information
1. Intern information
2. Personuppgifter eller information om anställda
3. Affärshemlig information
4. Särskild sekretessbelagd information ex, rörande rikets säkerhet.
   (sparas ej i Evados miljö utan i kundens egen miljö eller program)

Riktighet, används för att kontrollera att information, tjänster, produkter eller program har rätt information, fungerar korrekt och hög driftsäkerhet. Används för att säkerställa att dokument och information som skapas eller lagras är korrekt. Är ett bedömningsvärde som görs vid granskning av färdiga dokument, information som ska användas externt eller produkter. Används även som allvarlighetsgrad för systemfel eller supportärenden för våra produkter.

0. Planering, korrekt information
1. Normalt, mindre justeringar behöver göras
2. Viktigt, förändringar behöver göras
3. Allvarligt, förändringar behöver göras omgående
4. Kritiskt, förändringar behöver göras akut

Tillgänglighet, behörighetsstyrning som sker via lagringsmiljö av information och styrning genom behörighet till informationen.

0. **Öppen information**.
   Marknadsföring, information på sociala medier, hemsida, appar, kontaktuppgifter arbete anställda. Informationen är öppen för alla.
1. **Internt**
   Interna dokument, marknadsbevakning, statistik, delade dokument med återförsäljare. Information kräver inloggning med Office 365 konto.
2. **Affärshemlig**
   Personuppgifter, avtal, offerter, affärsplan, produktutveckling, uppgifter om egen personal. Information kräver inloggning med Office 365 konto.
3. **Personal**
   Känslig information om personal exempelvis anställningsavtal. Information kräver inloggning med Bank-ID
4. **Nationell nivå**
   Information som gäller rikets säkerhet, kommer ej hanteras i Evados miljö utan har kunden detta krav kommer kundens egen miljö och program att användas.

2 Informationshantering

Informationshantering på Evado kommer följa dessa riktlinjer och rutiner som beskrivs i detta kapitel. För att det ska passa alla är detta ramen och krav att uppnå sen har avdelningar, användargrupper eller områden möjlighet att komplettera med mer detaljerade och unika rutiner som behövs för deras arbete.
Hantering av information och lagring av information följs åt och detta kapitel kommer vi hänvisa till lagringsplatser som förklaras i avsnitt 3 Fillagring.

2.1 Allmänt

- All information ska sparas i molnlösning enligt anvisning i avsnitt 3 Fillagring.
- Informationen sparas bara så länge det finns ett tydligt syfte och enbart den information som finns behov av, finns inte detta ska informationen raderas. Följs upp två gånger per år av ansvarig och årligen av förvaltningsansvarig.
- Alla dokument ska skaps enligt Evadomall som finns upplagt, finns det inte en mall kontakta en systemadministratör eller förvaltningsansvarig.
- Evado tillhandahåller verktyg och program för att personal klarar av arbetsuppgifterna. Dock ifall anställda behöver använda sig av andra verktyg/program möjliggörs detta, förutsatt att rutiner för informationshantering följs.

2.2 Mail

- Mail som är äldre än 1 år raderas. Behöver informationen sparas längre, gör om till dokument och lagra under företagsmapp.
- Mail tillhörande projekt läggs i mapp och information hanteras vid projektavslut. Information som behöver flyttas läggs i anteckning/dokument och sparas under kundens namn.
- Filer som skickas via mail ska läggas in i projektgrupp eller användargrupp i Teams/SharePoint och radera mailet när detta är gjort.
- All internkommunikation ska ske via Teams undantaget är om mail ska skickas vidare till rätt person som ska svara på mailet direkt till kund.
- Ansvaret för hantering av information via mail är upp till varje anställd att följa rutiner och anvisningar. Systemadministratör eller förvaltningsansvarig har rättigheter att gå in och ta bort om anställda inte följer anvisningar.
- Privata mailkorgar tillåts i Outlook så länge mapparna är tydligt uppmärkt och skickas privata mail så gäller samma regler som arbetsrelaterade mail.

2.3 Microsoft Teams

- Används för samtlig intern kommunikation såsom chatt, videolösning och informationsspridning.
- Användargrupp är interna grupper och innehåller enbart intern information och skapas av förvaltningsansvarig.
- Projektgrupper skapas för samtliga interna och externa projekt. Projektgrupperna kan ha kunduppgifter och annan information som bara behövs för projektet. Projektgrupper raderas när projekt avslutas.
- Projektgruppen skapas av områdesansvarig i samråd med förvaltningsansvarig.
- För åtkomst av information på Teams behöver du vara inloggad med Office 365-konto och vara medlem i Teamsgruppen som har informationen.

2.4 Anteckningar

- Anteckningar skapas i varje användargrupp/projektgrupp samt privat och följer mall för hur nya flikar ska skapas.
- Anteckningar från projekt kontrolleras, rensas och sparas in under företagsmapp på lagringsplats. Information från projekt som ska in i användargrupp eller interna dokument ska läggas in i rätt användargrupp.

2.5 Formulär (kvantitativ datainsamling)

- Formulär används till att kontrollera att vi ställt rätt frågor vid säljmöten, utbildningar och utvärderingar. Vi använder Forms, används annat program skall informationen skrivas in i rätt dokument för att få rätt statistik och sedan raderas.
- Formulär för statistik sparas i rätt användargrupp och kontrolleras av ansvarig varje kvartal. Statistik sparas utan personuppgifter eller annan känslig information. Finns denna information med ska den raderas omgående. Kontakta systemadministratör eller förvaltningsansvarig vid problem.

2.6 Kvalitativ datainsamling

- Intervjuer används för mer kvalitativa insamlingar, t ex utlåtande om produkter från kunder eller kunniga inom området.
- Vid intervjuer så skall det finnas med ett godkännande från den intervjuade. Spelas intervjun in ska det finnas med ett muntliggodkännande på inspelningen och vilket syfte inspelningen har.
- Är intervjun enbart för anteckningssyfte ska intervjun raderas när anteckningen inte behövs oavsett om det är via text eller ljudinspelning.
- Är det information som vi behöver för att utveckla produkter, marknadsföring eller referensprojekt så sparas information i företagsmappen. Samt att den information som ska användas för internt bruk kopieras, redigeras och läggs in i rätt användargrupper.

2.7 Personlig informationshantering

- Eget ansvar att sköta mail, anteckningar och dokument enligt anvisning.
- Uppstår det problem eller behov av andra verktyg för att lösa sina arbetsuppgifter kontaktas närmsta chef och sedan förvaltningsansvarig.
- Vid nytt verktyg/ arbetssätt skickas information till förvaltningsansvarig som uppdaterar dokumentet: *Dokumentation av information - GDPR.*
- Upptäckts problem ska meddelande till systemadministratör och förvaltningsansvarig skickas med information om problem samt vilka/vad som påverkas.

2.8 HR

- Personal:
    - Interna policys skrivs om årligen och sparas i : *Dokumentation av information - GDPR.*
    - All information om personal och deras anhöriga (kontakt vid olyckor) sparas i Grant Thorntons lagringsmiljö och uppdateras av ansvarig kontinuerligt samt kontrolleras årligen.
    - Samtycke för användning av foton, intervjuer m.m. som inte krävs för att lösa sin arbetsuppgift ska årligen uppdateras och tydligt framgå att det är valfritt.
    - Kontaktuppgifter för arbetet, mail och telefonnummer sparas i Office 365 för att enkelt hitta internt men även kunna ge vidare till kunder vid behov.
- Rekrytering:
    - Vid rekrytering skapas en tillfällig mapp upp för ändamålet i Grant Thorntons lagringsmiljö. Där all information sparas i form av CV, personligt brev och andra dokument. Sparas så länge rekrytering pågår och raderas efter avslutad process.
    - Kommunikation sker via mail och sparas i mapp så länge rekryteringen pågår och raderas efter avslutad process.

- Personer som anses intressanta men inte blev anställda får förfrågan om vi får spara deras uppgifter till framtida rekryteringar. Personen behöver ge samtycke för att vi ska spara information och förnyas årligen annars raderas uppgifterna.

2.9 Sociala medier

- Inlägg på sociala medier, Instagram, Facebook och LinkedIn sker med syfte att informera om verksamheten och inte om enskilda individer även om inlägg kan anses personliga. Sociala medier används för att guida trafik till hemsidan samt att öka och bibehålla varumärkeskännedom.
- Publicering av bilder samt uppgifter av anställda med syfte att informera om verksamheten sker i samtycke med den anställde. Uppgifter som publiceras godkänns av personen i fråga och ska enbart innehålla information som är användbar för verksamheten och dess kunder.
- Kontaktuppgifter som publiceras ska enbart vara i professionellt syfte. Vi publicerar inte privat mail, telefonnummer, hemadress eller sådant som kan påverka den anställdas privatliv.
- Vill den anställde att uppgifter tas bort, tex bild, sker detta i samråd med verksamheten. Kontaktuppgifter (ej privata) till säljare eller produktansvarig kan vara nödvändiga för att kunna genomföra arbetsuppgifter.
- Inlägg med individer som inte är anställda på företaget, tex bilder från mässor eller seminarier sker i samtycke med berörda. Dessa inlägg används för att informera om verksamheten samt i marknadsföringssyfte.
- Bilder som läggs ut ska i största möjliga mån inte föreställa enskilda individer utan grupper vid tex mingel eller mässor.
- Personuppgifter utöver bilder ska undvikas så länge det inte är nödvändigt för innehållet.
- Vill en individ att inlägget ska raderas görs detta efter kontakt med Evado och ansvarig på Evado för inlägget.

2.10 Hemsidan

- Hemsidan används för att informera om Evados produkter, tjänster samt vad som händer inom verksamheten och relevant omvärldsbevakning.
- Personuppgifter på hemsidan publiceras då företaget kan motivera att det är viktigt att publicera uppgifterna. Till exempel om den anställda är chef eller har kundorienterade arbetsuppgifter eller produktansvar som gör det viktigt att göre den anställde tillgänglig att kontakta för kunder, potentiella kunder och medarbetspartners.
- Publicering av bilder på anställda sker alltid i samtycke med den berörde oavsett roll i företaget.

2.11 Nyhetsbrev

- Nyhetsbrev skickas till personer som gett sitt samtycke att prenumerera på brevet.
- Prenumerationen kan avslutas när som helst och då kontaktas ansvarig på Evado för avslut av nyhetsbrev.
- I samband med avslutad prenumeration tas personuppgifter såsom mail, namn och företag bort.

2.12 Sälj

- Säljarbete innan avtal:

    - Genomförda säljbesök och möten, affärsmöjligheter, kontaktuppgifter, delar information med återförsäljare kring dessa.
    - Skrivna offerter, förslag. Tas bort efter ett år eller om kunden väljer annan leverantör. Sparas i mapp som beskrivs i avsnitt 3 Fillagring nedan.
    - Uppföljning av gemensamt säljarbete i planeringsverktyg, raderas efter vunnen affär eller inget intresse och kontrolleras årligen.
- Säljarbete efter avtal:
    - Skriva avtal, sparas 3 år efter avslutat avtal i anvisad mapp enligt avsnitt 3 Fillagring.
    - Kontaktuppgifter används för fortsatt samarbete, merförsäljning av nya tjänster samt gemensamt utvecklande av affärer med berörd återförsäljare. För att säkerställa att kunden är okej med detta frågar vi efter samtycke vid uppdateringar av avtal eller årligen.
    - Överlämning av information vid övergång till projektfas sker vid vunnen affär. Där information lämnas över till Projektledare som skapar projektgrupp där all information läggs in för projektet även information som skrivits i mail.
    - Säljaren gör om anteckningar, dokument eller annan information som ska användas internt och lägger in detta i användargrupp. Uppgifter som berör kund och inte drivs vidare i projekt ska sparas under företagsmapp och CRM program vid behov. Resterande uppgifter raderas.

2.13 Projekt

- Projektgrupp:
    - Projektgrupp skapas i Teams/ SharePoint som används för kommunikation och lagring av information i projektet. Kan inte externa använda Teams delas dokument från SharePoint sidan och kommunikation via mail.
    - Projektledaren bekräftar att all information kommit in i projektgruppen från sälj och bjuder in de personer som ska vara med i projektet.
    - Projektgrupp ska alltid skapas oavsett om det är en stor projektgrupp eller enbart en person i projektet.
- Leveransutveckling:
    - När Workshop och informationsinsamling är genomförd skickas informationen vidare till leveransutveckling som bygger lösningen. Ärende om vad som ska göras skapas i Jira. Inga personuppgifter läggs in här som har extern koppling.
- Avslutning av projekt och överlämning till förvaltning:
    - Projektledaren utvärderar projektet och gör en sammanställning. Information som ska sparas flyttas över till Företagsmapp se avsnitt 3 Fillagring.
    - Annan information som ska sparas anonymiseras och flyttas över till rätt användargrupp i Teams/SharePoint. När det är gjort raderas projektgruppen och all information.

2.14 Support

- Support skickas in till Teamsgrupp Support. Meddelandet ska innehålla ifyllt formulär *felmeddelande produkt* om det gäller våra produkter för att supportärendet ska börja.
- Andra frågor går via *fråga säljare* om det är frågor om försäljning, fakturor eller vill veta mer om produkterna. Säljare eller leveransansvarig tar tag i ärendet.

- Extern kommunikation sker via mail och kund informeras att ärende kommit in, ärendet påbörjas och kund meddelas de åtgärder som behöver göras och uppskattad tidsplan. När ärendet är klart skickas nytt mail till kund och ärendet avslutas.
- Information kontrolleras och säkerställs att inga känsliga personuppgifter finns med. Skulle detta inträffa görs en kopia utan dessa uppgifter och originalet raderas. Information från kund stannar i Supportgruppen tills ärendet är löst. Nödvändig information från supportgruppen och mail kopplat till ärendet sparas sedan under mappen företag och raderas från Supportgruppen/ mail.
- Möjlighet att lämna supportärende finns även via telefon och då fyller den som svarar i formulär *felmeddelande produkt* eller hänvisar till rätt person beroende på ärendet.

2.15 Uppföljning

- Uppföljning av informationshantering och fillagring sker en gång per år av Förvaltningsansvarig. Samtliga ansvarig för projektgrupper, användargrupper och områdesansvariga är inblandade och gör en inventering av information som de har ansvar över.
- Innan uppföljning finns ett revideringsfönster av styrdokument för att se att det är aktuellt och ger rätt effekt för företaget.
- Varje ansvarig gör varje halvår en kontroll för att säkerställa att rutiner följs och att vi har korrekt information.
- Uppföljning och kontroller görs löpande i användargrupper, projektgrupper och per anställd i det dagliga arbetet enligt rutiner som finns.
- Uppföljning och kontroll loggas i dokument: *Dokumentation av information - GDPR*

2.16 Säkerhet

Säkerhet delas in i lösenordshantering, enheter och skalskydd. Säkerhet om lagringsplats, externa system eller egna produkter beskrivs längre ner i dokumentet i avsnitt 3 Fillagring.

2.16.1 Lösenord

- Inloggningsuppgifter till företagets program, miljö eller verktyg ska sparas i Evados lösenordshanteringsprogram vid behov. Alternativt att de sparas i enhetens eget lösenordshanteringsprogram.
- Admin eller lösenord till kundappar m.m. ska alltid sparas i lösenordshanteringsprogram.

2.16.2 Enheter

- Enheter är exempelvis, smartphones, smart watch, tablets och datorer.
- Dessa ska gå att rensa från distans, personal ansvarar för detta själv.
- Alla enheter ska vara lösenordskyddade/skyddade (Skalskydd).
- Samtlig information som är företagsrelaterat ska sparas i moln-lagring och kontinuerligt rensas lokalt från enhet, förslagsvis varje månad men minst en gång i kvartalet. Med undantag för information som behövs för utveckling av exempelvis kod, behöver ej kontinuerligt rensas.

2.16.3 Skalskydd

- Kontorslokalen är larmad och låst utanför kontorstid. Under kontorstid krävs antingen nyckel eller passerkort för att komma in i lokalen.

- Alla servrar som erbjuder publika tjänster tillhandahålls av molnleverantörer som själva ansvarar för skalskydd till deras serverhallar mm. Servrar som används för test, demo och utveckling finns både i molnet och på kontoret. Servrar på kontoret skyddas dels av lokalens larm och lås, och dels av inloggning med användarnamn och lösenord.
- Samtliga servrar, i molnet och på kontoret, skyddas av brandväggar. Servrarna kan nås enbart på de sätt som krävs för att tillhandahålla publika tjänster, eller för att möjliggöra intern administration och övervakning. I det senare fallet krävs användarnamn och lösenord för åtkomst.

2.17 Säkerhetskopior

- Säkerhetskopior av våra interna program och dokument:
    - Alla system, program och dokument ska säkerhetskopieras i molnet och molntjänsten ska erbjudas av systemleverantören.
    - Det ska tydligt framgå i registret/protokollet för våra program och system hur säkerhetskopior görs och hur länge de sparas.
- Säkerhetskopior av våra produkter och system som vi ansvarar för:
    - Evados system och lösningar som vi ansvarar internt eller åt kund säkerhetskopieras regelbundet.

3 Fillagring

På Evado använder vi oss av Office 365 lösning för hantering av filer. Vi använder Teams och SharePoint för användargrupper och projektgrupper. För lagring av filer används Onedrive. Sparade dokument skall ha tydligt syfte som stärker behovet av lagringen. Förvaltningsansvarig har övergripande ansvar och delegeras ner till ägare av användargrupp, projektgrupp eller privat mapp.

3.1 Användargrupper och projektgrupper

Nedan följer beskrivning av användargrupp och projektgrupp. Dessa skapas i Teams och SharePoint och möjliggör snabb tillgång till rätt information för arbetsuppgifterna i olika grupper.

3.1.1 Användargrupp

Lösning för snabbt åtkomst av relevant information till uppgiften som ska göras. Tillgång till grupperna styrs gruppägare, systemadministratör eller förvaltningsansvarig. Alla dokument för internt bruk ska läggas in via användargrupp. Alla dokument från användargrupper synkas till mapp ”Evado” på Onedrive. För att ha åtkomst behöver du vara inloggad med Office 365 konto.

3.1.2 Projektgrupp

Skapas för varje projekt på företaget både internt och externt. Anställda och andra personer som är med i projektet läggs in som medlemmar i gruppen. Projektgrupper har inte automatisk synkning utan när projektet stängs görs en utvärdering och sammanställning av projektet, för att säkerställa att fel information inte lagras. När projekt avslutas går projektledaren igenom filer och information för att säkerställa att det finns ett tydligt syfte att spara informationen. Dokumentet flyttas sedan till mapp ”företag”, läggs in under företagets namn och vid internt bruk flyttas dokument till rätt användargrupp. Åtkomst styrs via inloggning med Office 365 konto.

3.2 Lagring

All fillagring är inte praktiskt att ha i användargrupper eller projektgrupper och sparas därför i lagringsmappar. Information som behöver sparas för avtal, information om egen personal och

sekretess belagda dokument sparas i lagringsmappar. Samt synkning mellan användargrupper och mapp Evado möjliggör delning av information mellan olika områden i företaget.

3.2.1 Grant Thornton

Information som rör personal, lagras på annan molnlagring av Grant Thornton som styr rättigheterna att se dokument via anställningsavtal samt bakom inloggning via BankID.

3.2.2 Företagsmappar

All information om våra kunder, återförsäljare eller återförsäljares kunder lagras under mappen Företag. Varje företag har en mapp där all information som rör företaget lagras.
För att komma åt mappar på lagringsplats krävs att du har fått tillgång till denna mapp via Förvaltningsansvarig eller systemadministratör i Office 365. Inloggning sker via Office 365 konto.

3.2.3 Evado

Interna dokument oavsett avdelning på företaget. Dessa dokument synkas från användargrupper automatiskt. Inga dokument läggs in direkt i mappen utan ska läggas in via användargrupper i Teams/SharePoint. Alla som är anställda på Evado kommer ha tillgång till denna mapp om de är inloggade med deras Office 365 konto.

3.2.4 Privat

Under lagringsplats privat är personalens egna dokument som inte är färdiga för att dela i användargrupper/projektgrupper. Genom att erbjuda denna lösning sparas inga filer eller information lokalt på enheten utan allt sparas i molnet. Enbart personen själv som har åtkomst till denna mapp och kan själva styra att dela dokument och mappar med andra. För att kunna använda mappen krävs inloggning med Office 365 konto.

4 Hantering av personuppgifter

Hantering av personuppgifter har samma rutiner som hantering av information på Evado, där vi beslutat att använda anvisningar från GDPR och lagt det som grund för informationshantering.

4.1 Inventering av personuppgifter

Vi arbetar systematiskt med att uppdatera vårt register för personuppgifter. Registret sparas i Grant Thorntons miljö med BankID som inloggning. Det är enbart administratörerna som kommer åt detta dokument. För att se hur registret ser ut fråga se dokument: *Dokumentation av information – GDPR*. Vid behov av granskning, kontakta förvaltningsansvarig.

4.1.1 Kategorisering av personuppgifter

För att få överblick och enklare hantera externa personuppgifter som vi hanterar delar vi in dem i kategorier. Kategori 1-4 avser information som hanteras i våra produkter medan kategori 5-7 är information som rör egen personal eller är kundrelaterade.
Känsliga personuppgifter, kan förekomma internt på företaget för att ha koll på personalshälsa om det finns behov för att kunna ge stöd och hjälp, det är personen själv som beslutar vilka som får veta informationen annars är det enbart personens chefer som hanterar uppgifterna. Känsliga personuppgifter som är externa hanteras genom att det som klassas som känsligt raderas.

1. **Användarinformation**

- Förnamn, Efternamn, E-post, Telefonnummer, Adress, Postnr, Personnummer, Användar-ID och Passord (krypterad).

2. **Slutkundsinformation**
   - Förnamn, Efternamn, E-post, Telefonnummer, Adress, Användar-ID, Passord (krypterad).
3. **Anläggningsinformation**
   - Anläggnings ID, MätarID, Portkod, Protokoll.
4. **Teknikinformation**
   - IP nummer, Telefonmodell.
5. **Personalinformation**
   - Förnamn, Efternamn, Personnummer, Telefonnummer, E-post, Adress, Postnr, Anställningsavtal, Lönespecifikation, Utvecklingsplan.
6. **Kundinformation (Återförsäljare, Egna kunder och Kunder via återförsäljare)**
   - Förnamn, Efternamn, E-post, Telefonnummer, Personnummer, Adress, Foton

4.1.2 Egna produkter där personuppgifter behandlas

Beskrivning av varje produkt finns i respektive produktbeskrivning: *Produktbeskrivning produktnamn*

4.1.2.1 Evado Arbetsorder

Produkten behandlar personuppgifter inom kategori 1, 2, 3, och 4.

4.1.2.2 Evado Mätarbyten

Produkten behandlar personuppgifter inom kategori 1, 2, 3, och 4.

4.1.2.3 Evado Mobile Core

Produkten behandlar personuppgifter inom kategori 1, 2, 3, och 4.

4.1.2.4 Evado RecoVR

Produkten behandlar inga personuppgifter.

4.1.2.5 Evado Transportsystem

Produkten behandlar personuppgifter inom kategori 1, 2 och 4 .

4.1.3 Program Evado använder och personuppgifter behandlas

Personuppgifter behandlas i flera program för att vi ska klara av vår verksamhet. För mer detaljerad information om vad programmen används till och vilka uppgifter som sparas se dokument: *Dokumentation av information - GDPR.*

4.1.3.1 Allmänt

- QBIS projektsystem
  Hanterar personuppgifter från kategori 5 och 6.
- Office 365; Exchange, OneDrive, OneNote, SharePoint, Teams, Planner, Outlook, Excel, Word, Power Point, Skype för företag.
  Hanterar personuppgifter från kategori 5 & 6 och i vissa fall 1& 2 men ovanligt.

4.1.3.2 Projektledningsverktyg och CRM

- SmartSheet, Podio och Vidyo,
  Hanterar personuppgifter från kategori 5 & 6.

4.1.3.3 Utvecklingsverktyg

- Jira, Git och Confluens, hanterar i vissa fall personuppgifter från kategori 1,2,3 & 4 men är ovanligt. Utan är främst från kategori 5, för att kunna använda programmen.

4.2 Rättslig grund att spara personuppgifter

Olika grunder att spara information beskrivs i detta avsnitt. Även förpliktelser, samtycke och intresseavvägningar ingår under detta avsnitt.

4.2.1 Avtal

Ett avtal kan utgöra en rättslig grund för att behandla personuppgifter. Det krävs då att behandlingen är nödvändig för att fullgöra ett avtal med den registrerade eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås. Det gäller bara sådana avtal i vilka den registrerade är eller avser att bli part. Exempel på personuppgiftsbehandling som kan vara nödvändig i samband med avtal är kund- och personaladministrativa system för bland annat fakturering respektive löneberäkning.

4.2.1.1 Avtalstyper i Evado

- Finansiella avtal med finansiärer såsom aktieägaravtal, investeringsavtal, reversavtal, konvertibelavtal, låneavtal)
- Anställningsavtal för personal
- Underkonsultavtal för affärsutveckling
- Återförsäljaravtal för mobila produkter
- Partneravtal
- NDA och sekretessavtal
- Kundavtal (innehåller SLA bilaga)
- Personuppgiftsbiträdesavtal
- Personuppgiftsbiträdesavtal i affärer där vi samverkar med överliggande system såsom CGI och EG Sverige ska primärt återförsäljaren teckna personuppgiftbiträdesavtal mellan kund och systemägare. Evado ska teckna mellan återförsäljaren och Evado.

4.2.1.2 Hur länge ska avtalen sparas?

De ska sparas under hela avtalsperioden samt 1 år efter avtalsperiodens slut. Avtal får ej raderas utan avtalsägarens godkännande (inom Evado). Avtal som inte har en avtalsperiod utan mer tillsvidare ska ej raderas.

4.2.2 Rättslig förpliktelse

Personuppgifter får behandlas om det är nödvändigt för att uppfylla en rättslig förpliktelse. Den rättsliga förpliktelsen ska åligga den personuppgiftsansvarige och följa av EU-rätt eller svensk rätt. Som exempel på en rättslig förpliktelse kan nämnas bokföringsskyldigheten som anges i bokföringslagen.

4.2.3 Samtycke

Personuppgifter får behandlas om man har ett samtycke från den som personuppgifterna avser. I dataskyddsförordningen ställs det särskilda krav på samtycket, bland annat att det ska vara frivilligt, att det ska lämnas genom ett uttalande eller en entydig bekräftande handling och att det ska ges efter att den registrerade har fått information om personuppgiftsbehandlingen.

- Samtycke skickas till kund, där kunden svarar för att säkerställa att kontaktuppgifter, får användas exempelvis inom marknadsföring, fortsätt säljverksamhet samt referenssyfte. Lagras i dokument: *Dokumentation av information – GDPR*.
- Samtycke gäller fram tills att kunden tar tillbaka samtycke. För att det inte ska blir bortglömt så uppdateras samtyckesavtal årligen i samband med den årliga uppföljningen.
- Om samtycke inte finns är det möjligt att gå vidare i arbetet om en intresseavvägning görs men vi föredrar att kunden gett sitt samtycke.

4.2.4 Intresseavvägning

Det kan vara tillåtet att behandla personuppgifter efter en intresseavvägning. Det krävs då att behandlingen är nödvändig för berättigade intressen och att den registrerades intresse av skydd för sina personuppgifter inte väger tyngre. Barn anses vara särskilt skyddsvärda.

- För att gå vidare med arbetet med grund av intresseavvägning ska den göras skriftligt och dokumenteras i dokument *Dokumentation av information – GDPR*.
- Innan intresseavvägning används kontrollera om det finns grund i avtal eller samtycke, då ska det väljas istället.

5 Konsekvensbeskrivning

Begreppet personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Vi arbetar med konsekvensbedömning vid varje incident för att säkerställa vilka åtgärder som ska göras. Vi skriver in värdena från KLASSA, som ger oss typ av information, vilken skyddsklass och allvarlighetsgraden som rör incidenten. Detta kompletteras med riskbedömning och läggs in i en matris för att få en överskådlig bild. Efter det görs en konsekvensanalys och beslutar direkta åtgärder, långsiktiga åtgärder och hur detta ska förhindras i framtiden. När detta är klart informeras de som är påverkade av incidenteten. Även rapportering enligt rapporteringsskyldighet som beskrivs i nästa stycke.

6 Rapporteringsskyldighet

Om vi blir utsatta för dataintrång eller på något annat sätt förlorar kontrollen över de uppgifter vi behandlar, en så kallad personuppgiftsincident, måste vi utan onödigt dröjsmål underrätta den personuppgiftsansvarige om detta. Detta kallas rapporteringsskyldighet.

- Internt ska systemadministratör för system kontaktas, närmsta chef och förvaltningsansvarig så fort ett fel upptäckts som är nivå 2-4. Nivå 0-1 rapporteras in via Teams: Support.
- Påverkas felet externt ska leveransansvarig och säljansvarig kontaktas för att meddela vidare. Beskrivning av felet samt plan på åtgärder ska finnas. Gäller det återförsäljare eller kunder via återförsäljare följs anvisningar som finns i återförsäljaravtalet.

- Vid intrång ska datainspektionen kontaktas inom 72 h förutom dataskyddsinspektionen meddelar vi personuppgiftsansvarig och personbiträdet att intrång har inträffat, riskanalys och vad som görs för att åtgärda problemet. Det är i sin tur personuppgiftsbiträdet som avgör om meddelande ska ut till användaren/användarna som berörs av intrånget.
    - Informationen ska innehålla uppgifter om
        - Vilken typ av incident det är fråga om?
        - Vilka kategorier av personer som kan komma att beröras?
        - Hur många personer det berör?
        - Vilka konsekvenser incidenten kan få?
        - Vilka åtgärder man vidtagit för att motverka ev. negativa konsekvenser?