Vad innebär det för stödmottagaren att vara ett personuppgiftsbiträde i program inom Erasmus+ och Europeiska solidaritetskåren?

1. **Agera på uppdrag**: Du får endast behandla personuppgifter som uppfyller de ändamål som beskrivs i meddelandet om skydd av personuppgifter som finns tillgängligt på https://ec.europa.eu/erasmus-esc-personal-data. Om du behandlar personuppgifterna för egna ändamål går du utanför din roll som personuppgiftsbiträde och blir personuppgiftsansvarig för denna behandling. En beskrivning av huvudaktörerna ges längre fram i detta dokument.

2. **Bunden av ett avtal:** Du har ett bidragsavtal med ett nationellt programkontor för Erasmus+ eller Europeiska solidaritetskåren som beskriver dina skyldigheter som personuppgiftsbiträde. Detta avtal fastställer den rättsliga ramen för din roll som personuppgiftsbiträde, i överensstämmelse med förordning 2018/1725 där personuppgiftsbiträdets skyldigheter förklaras i artikel 29.

3. **Användning av underentreprenörer**: Du får inte anlita ett annat personuppgiftsbiträde utan skriftligt förhandstillstånd från den personuppgiftsansvarige. Kontakta den personuppgiftsansvarige för mer information om detta ämne. Du hittar kontaktuppgifter till den personuppgiftsansvarige i meddelandet om skydd för personuppgifter. Sätt ditt nationella programkontor i kopia för denna kommunikation.

4. **Tillämpning av datasäkerhet**: Du måste införa tekniska och organisatoriska åtgärder som är lämpliga i förhållande till risken för behandlingen för att garantera säkerheten för personuppgifter, inbegripet oavsiktlig eller olaglig förstöring eller förlust, ändring, obehörig utlämning eller obehörig åtkomst. (Se checklistan för säkerhet nedan.)

5. **Anmälan av personuppgiftsincidenter**: Om du blir medveten om att en personuppgiftsincident har inträffat måste du anmäla det till den personuppgiftsansvarige utan onödigt dröjsmål. Du måste också hjälpa den personuppgiftsansvarige att uppfylla sina skyldigheter i samband med personuppgiftsincidenter genom att tillhandahålla all nödvändig information om incidenten, vilka steg som redan har vidtagits för att begränsa incidenten samt bedöma de sannolika konsekvenserna för de registrerade. Du hittar kontaktuppgifter till den personuppgiftsansvarige i meddelandet om skydd för personuppgifter. Sätt ditt nationella programkontor i kopia för denna kommunikation.

6. **Informera om potentiella överträdelser av personuppgiftsskyddet**: Du måste informera den personuppgiftsansvarige omedelbart om ändamålen och medlen för en behandling skulle kunna leda till en överträdelse av förordning (EU) 2018/1725 eller nationell dataskyddslagstiftning.

7. **Vara ansvarsskyldig**: Du måste uppfylla dina ansvarsskyldigheter, till exempel ta fram och införa strategier för dataskydd (strategier som inför en standard för användning, övervakning och hantering av personuppgifter i din organisation), dokumentera din uppgiftsbehandling (bifogat finns en exempelmall för register över kategorier av behandling).

8. **Begränsning av internationella överföringar**: Dataskyddsförordningen har mycket strikta regler för överföring av personuppgifter till tredjeländer. Du måste säkerställa att den personuppgiftsansvarige har godkänt en eventuell överföring utanför EU/EEA, utöver de överföringar som definierats i bidragsavtalet med det nationella programkontoret för Erasmus+ eller Europeiska solidaritetskåren, och att överföringen överensstämmer med förordningens bestämmelser om internationella dataöverföringar. Detta rör situationer där du överför data direkt, utan stöd av Europeiska kommissionens IT-verktyg, till andra organisationer utanför EU/EEA eller när du beviljar sådana organisationer åtkomst i Europeiska kommissionens IT-verktyg. Kontakta den personuppgiftsansvarige för mer information om detta ämne. Du hittar kontaktuppgifter till den personuppgiftsansvarige i meddelandet om skydd för personuppgifter. Sätt ditt nationella programkontor i kopia för denna kommunikation.

Checklista för säkerhet

- ✓ **Vi förstår kraven på konfidentialitet, integritet, tillgänglighet och motståndskraft** hos de system och tjänster där uppgifterna behandlas.

    - **Konfidentialitet** liknar sekretess. Åtgärder för konfidentialitet är utformade för att förhindra obehörig åtkomst till känslig information.

    - **Integritet** inbegriper att bevara uppgifternas konsistens, riktighet och tillförlitlighet genom hela sin livscykel. Uppgifterna får inte ändras vid överföring, och du måste vidta åtgärder för att säkerställa att uppgifterna inte kan ändras av obehöriga personer (till exempel vid ett brott mot konfidentialiteten).

    - **Tillgänglighet** innebär att information ska vara konsekvent och lättillgänglig för behöriga parter. Det här kravet innebär lämpligt underhåll av hårdvara, teknisk infrastruktur och system för lagring och visning av uppgifterna.

    - **Motståndskraft** handlar om din organisations förmåga att fortsätta driva verksamheten vid en störning och dess förmåga att återställa sina system till funktionsdugligt skick inom "rimlig tid"**.**

- ✓ **Vi känner till vilka som har tillgång till de uppgifter vi ansvarar för** och vi kontrollerar regelbundet listan med behöriga personer. Detta gäller både för IT-verktyg som tillhandahålls av Europeiska kommissionen och IT-verktyg som vi själva använder. Personerna omfattas av en lämplig lagstadgad tystnadsplikt.

- ✓ **Vi överför endast uppgifterna via säkra överföringsprotokoll** (till exempel säkra internetanslutningar, men inte via e-post – om den inte är krypterad)**.**

- ✓ **Vi lagrar uppgifter på säkra platser** när vi exporterar uppgifterna från EU-kommissionens IT-verktyg, och säkerställer att endast behörig personal har tillgång till dem (bra exempel: lokal hårddisk på en lösenordsskyddad dator, nätverksenhet (filserver) med åtkomstskydd; dåliga exempel: lokal hårddisk på en offentligt tillgänglig dator, ett USB-minne, molnlagring – om inte din organisations säkerhetspolicy tillåter det).

- ✓ **Vi är medvetna om den begränsade lagringsperioden för uppgifterna** och när denna period är slut upphör vi med behandling av personuppgifter relaterade till de ändamål som definieras i meddelandet om skydd av personuppgifter utanför de IT-verktyg som tillhandahålls av Europeiska kommissionen.

Vilka är huvudaktörerna vid behandling av personuppgifter i programmen inom Erasmus+ och Europeiska solidaritetskåren?

För den uppgiftsbehandling som definieras i meddelandet om skydd av personuppgifter tillgängligt på https://ec.europa.eu/erasmus-esc-personal- data:

1. Europeiska kommissionen, generaldirektoratet för utbildning och kultur fungerar som **personuppgiftsansvarig**.

2. De nationella programkontoren för Erasmus+ och Europeiska solidaritetskåren fungerar som **personuppgiftsbiträden**.

3. Organisationer och enskilda personer som skriver under och övertar de rättigheter och skyldigheter som härrör från bidragsavtalet med de nationella programkontoren för Erasmus+ och Europeiska solidaritetskåren tar över rollen som **personuppgiftsbiträden** (även kallade underentreprenörer).