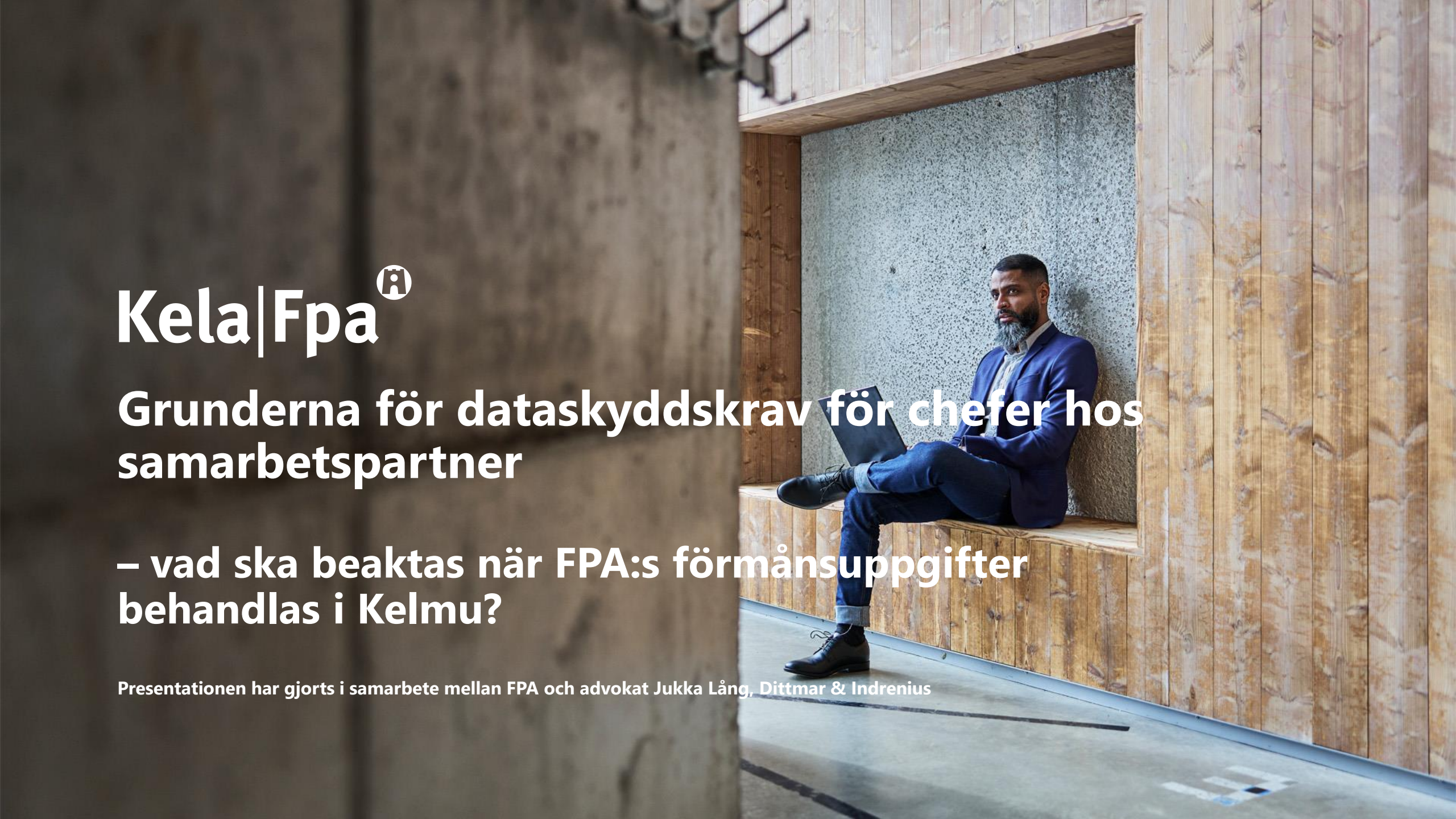


Kela|Fpa

Grunderna för dataskyddskrav för chefer hos samarbetspartner

– vad ska beaktas när FPA:s förmånsuppgifter behandlas i Kelmu?

Presentationen har gjorts i samarbete mellan FPA och advokat Jukka Lång, Dittmar & Indrenius

Inledning

Vad är dataskydd och varför är det viktigt?

- Var och en har rätt till skydd för sina personuppgifter (10 § i Finlands grundlag).
- Skyddet för personuppgifter (> dataskydd) är en grundläggande rättighet som säkerställer att den registrerades rättigheter och friheter tillgodoses vid behandlingen av personuppgifter.
- Bestämmelser om dataskydd finns i EU:s allmänna dataskyddsförordning och den nationella dataskyddslagen.
- Dataskyddet visar **när och under vilka förutsättningar personuppgifter kan behandlas**.
- En korrekt organisering av dataskyddet är inte bara en fråga om att uppfylla lagstadgade krav, utan också en del av en **ansvarsfull verksamhet**.
- **Datasäkerhet** är en praktisk åtgärd som syftar till att genomföra dataskyddet. Det handlar framför allt om att skydda informationens integritet och konfidentialitet med tekniska och organisatoriska medel.

Grundläggande begrepp i fråga om dataskydd

- **Personuppgifter** är alla uppgifter som hänför sig till en identifierad eller identifierbar fysisk person.
- **Behandling av personuppgifter** är alla åtgärder som gäller personuppgifter.
- **Registrerad** är den person som personuppgifterna gäller.
- **Personuppgiftsansvarig** är benämningen för en person, ett företag, en myndighet eller en sammanslutning som fastställer syftena och metoderna för behandlingen av personuppgifter. Den personuppgiftsansvarige har det övergripande ansvaret för behandlingen av personuppgifter.
  - Samarbetspartnerna är personuppgiftsansvariga när de behandlar personuppgifter som erhållits från FPA.
- **Personuppgiftsbiträdet** är en aktör som behandlar personuppgifter för den personuppgiftsansvariges räkning.
  - Personuppgiftsbiträdet handlar enligt den personuppgiftsansvariges anvisningar och under dennes överinseende.

Kela|Fpa

Samarbetspartnerns rätt att få uppgifter

- Samarbetspartnern har rätt att ta emot personuppgifter (bl.a. kundernas förmånsuppgifter) från FPA för att kunna genomföra sin verksamhet på ett ändamålsenligt sätt.
- Rätten att få uppgifter bygger på lagstiftning.
  - Samarbetspartnern har rätt att med stöd av speciallagstiftningen få de nödvändiga uppgifter som den behöver för att sköta sina uppgifter.
  - Informationsöverföringen mellan myndigheters informationssystem via tekniska gränssnitt baserar sig på 22 § i lagen om informationshantering inom den offentliga förvaltningen (906/2019).
- Speciallagarna, till exempel kunduppgiftslagen, gör det möjligt att få **nödvändig information** via FPA:s förmånsdatatjänst Kelmu. Samarbetspartnerna ska säkerställa kundernas integritetsskydd i fråga om erhållna uppgifter genom att uppfylla **skyldigheterna enligt dataskyddsförordningen**.
- Utlämnande av uppgifter definieras också i parternas **avtal om utlämnande av FPA:s förmånsuppgifter med hjälp av en teknisk anslutning**.

Kela|Fpa

De uppgifter som FPA lämnar ut är sekretessbelagda.
Samarbetspartnerna beviljar sina anställda Suomi.fi-fullmakt först efter att de anställda har fått **tillräckliga instruktioner om dataskydd och åtminstone tagit del av det här FPA-materialet.**
Samarbetspartnerna förbinder sig att övervaka och ansvara för att deras anställda som har användarrättighet använder informationssystemet och de uppgifter som erhållits via det i enlighet med avtalet mellan parterna.

Skyldigheter enligt dataskyddsförordningen

- Samarbetspartnerna behandlar personuppgifter som de tagit emot från FPA **i egenskap av personuppgiftsansvariga**, och de ska se till att
  - **principerna om dataskydd** vid behandling av personuppgifter följs och att detta påvisas
  - det finns en laglig **grund för behandlingen**
  - **de registrerades rättigheter** tillgodoses
  - tekniska och organisatoriska åtgärder införs för att säkerställa dataskydd och datasäkerhet
  - principerna för dataskydd genomförs
    - exempelvis interna anvisningar och tillvägagångssätt finns och tillämpas samt att utbildningar ordnas

Principer för dataskydd

Dataskyddsprinciperna ska följas alltid då personuppgifter behandlas. Den personuppgiftsansvarige ska också kunna visa att dataskyddsprinciperna tillämpas effektivt vid behandlingen av personuppgifter.

Kela|Fpa

Vilka principer finns det för dataskydd?

Laglighet, korrekthet och öppenhet

Ändamålsbegränsning

Uppgiftsminimering

Korrekthet

Lagringsminimering

Integritet och konfidentialitet

Ansvarsskyldighet

Principer för dataskydd 1/2

1. **Laglighet, korrekthet och öppenhet**
   - Behandlingen av personuppgifter ska uppfylla kraven i dataskyddslagstiftningen. Behandlingen ska ha en laglig grund och vara ändamålsenlig och skälig i förhållande till det ändamål som fastställts. Med öppenhet avses att den registrerade ska informeras på ett tydligt och begripligt sätt om behandlingen av personuppgifter och de rättigheter som är förenade med den före och under behandlingen.
2. **Ändamålsbegränsning**
   - Personuppgifter får behandlas endast för uttryckligt angivna och berättigade ändamål. Uppgifterna får användas endast för skötseln av de uppgifter som åläggs samarbetspartnern i lagstiftningen.
3. **Uppgiftsminimering**
   - Endast personuppgifter som är behövliga för behandlingen får behandlas. Det är samarbetspartnernas och deras anställdas ansvar att endast läsa behövliga uppgifter om varje kund.
4. **Korrekthet**
   - De personuppgifter som behandlas ska vara korrekta och uppdaterade. Inexakta och felaktiga personuppgifter ska rättas eller raderas utan dröjsmål.

Principer för dataskydd 2/2

5. Lagringsminimering

- Personuppgifter får bevaras endast så länge det är nödvändigt för uppgifternas användningsändamål. Den personuppgiftsansvarige ska planera och kunna motivera den lagringstid som tillämpas. Lagringstiderna för personuppgifter ska dokumenteras.

6. Integritet och konfidentialitet

- Behandlingen av personuppgifter ska vara konfidentiell och säker. Den personuppgiftsansvarige ska bedöma eventuella risker, nivån på organisationens dataskydds- och datasäkerhetsanvisningar samt det tekniska skyddet av personuppgifter. Rätten att ta del av uppgifter som lämnas ut genomförs i enlighet med avtalet på basis av stark autentisering (vid den tidpunkt då avtalet träder i kraft används Suomi.fi-identifikation).

7. Ansvarsskyldighet

- Den personuppgiftsansvarige ska kunna visa att den följer dataskyddsbestämmelserna och ska beakta dem redan under behandlingen av personuppgifter. Omfattningen av ansvarsskyldigheten beror på organisationens storlek, antalet personuppgifter och vilken typ av personuppgifter som den personuppgiftsansvarige behandlar. Om den personuppgiftsansvarige inte kan visa att den uppfyller dataskyddskraven, kan detta leda till administrativa påföljder.

Kela|Fpa

Ansvar och information – Information till registrerade

För att visa att den uppfyller sina skyldigheter i fråga om dataskydd ska den personuppgiftsansvarige informera de registrerade om följande:

- **Vilken** organisation som ansvarar för behandlingen
- (**Vilka** som behandlar uppgifterna)
- **Vilka** kontaktuppgifterna till organisationen och dess dataskyddsombud är
- **Varför** uppgifterna behandlas (ändamålet)
- **Vem** uppgifterna gäller
- **Vilka** uppgifter som behandlas
- **Varifrån** uppgifterna fås
- **Hur länge** uppgifterna lagras
- **Hur** de registrerade profileras/beslut automatiseras (logik)
- **Vilka** nackdelar behandlingen innebär för en enskild person
- **Om** det är obligatoriskt att lämna uppgifterna till organisationen
- **Till vem** (organisationer) uppgifterna lämnas
- **I vilket** land behandlingen utförs
- **I vilket** land uppgifterna lagras
- **Vilken** behandlingsgrund som ger rätt till behandlingen
- **Vilka** rättigheter de registrerade har (Vad man avser att berätta/vad som måste berättas för enskilda personer. Hur?)

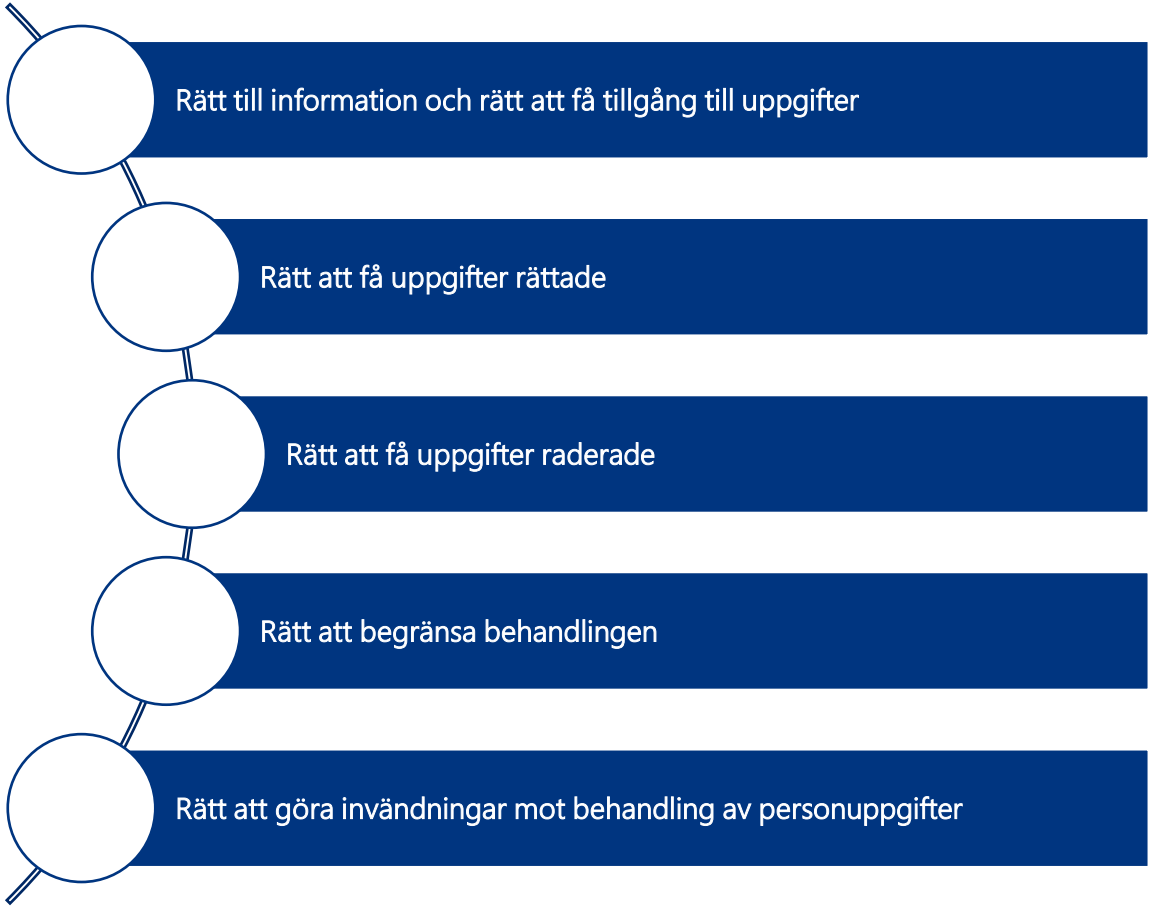
Kela|Fpa

Behandlingsgrunder

- Den personuppgiftsansvarige får behandla personuppgifter endast när det finns en laglig grund för behandlingen.
- Grunden för behandlingen begränsar de syften för vilka den personuppgiftsansvarige kan behandla (inkl. lämna ut) uppgifter.
- Samarbetspartnerna får inte lämna de erhållna uppgifterna vidare, såvida lagstiftningen inte kräver något annat.
- Behandlingsgrunden ska identifieras och fastställas innan behandlingen inleds, med avseende på alla olika behandlingsåtgärder.
- Behandlingsgrunden kan inte ändras medan behandlingen pågår.

Registrerades rättigheter

Tillgodoseende av den registrerades rättigheter



- Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att tillgodose de registrerades rättigheter.
- Utövandet av dessa rättigheter ska underlättas genom att praktiska förfaranden för utövandet av rättigheterna planeras och införs.

Registrerades rättigheter i praktiken

- **Rätt till information och rätt att få tillgång till uppgifter**
  - Den registrerade har rätt att veta om hens personuppgifter behandlas eller inte. Om uppgifterna behandlas ska en utredning över de personuppgifter som behandlas läggas fram för den registrerade.
- **Rätt att få uppgifter rättade**
  - Den registrerade har rätt att få felaktiga eller bristfälliga personuppgifter rättade.
- **Rätt att få uppgifter raderade**
  - "Rätten att bli bortglömd" innebär att den registrerade kan begära att personuppgifterna ska raderas när det inte finns något tvingande skäl för att behandla dem vidare.
- **Rätt att begränsa behandlingen**
  - Den registrerade har rätt att begränsa behandlingen av sina personuppgifter i vissa situationer. Om behandlingen begränsas ska den personuppgiftsansvarige eller personuppgiftsbiträdet ha rätt att lagra personuppgifterna, men inte att fortsätta behandla dem.
- **Rätt att göra invändningar mot behandling av uppgifter**
  - Den registrerade kan i vissa situationer ha rätt att göra invändningar mot behandlingen av sina personuppgifter, det vill säga begära att de inte alls behandlas. Den registrerade kan göra invändningar mot behandlingen av skäl som hänför sig till hens specifika situation.

Kela|Fpa

Den registrerades utövande av sina rättigheter

- Utöver att informera om den registrerades rättigheter ska den personuppgiftsansvarige göra det möjligt för den registrerade att utöva dessa rättigheter.
  - Informationen ska vara lättförståelig och tillgänglig på ett tydligt och enkelt språk.
- Behandlingen av personuppgifter ska ordnas så att begäranden från registrerade som vill utöva sina rättigheter kan besvaras effektivt.
- Den registrerades rättigheter bör också beaktas vid den tekniska planeringen av register och behandlingssystem.
- Det sätt på vilket den registrerade identifieras är mycket viktigt.
  - Den personuppgiftsansvarige har rätt att vägra besvara en begäran, om den kan visa att den inte kan identifiera den registrerade.

Kela|Fpa

Lämpliga arrangemang för datasäkerhet

Kela|Fpa

Datasäkerhetskraven enligt dataskyddsförordningen

- Artikel 32 i dataskyddsförordningen gäller skyldigheten att iaktta s**äkerhet i samband med behandlingen**.
- Den personuppgiftsansvarige ska vidta **lämpliga tekniska och organisatoriska åtgärder** för att säkerställa en säkerhetsnivå som är tillräcklig i förhållande till riskerna i samband med behandlingen.
  - Lämpliga åtgärder kan till exempel omfatta pseudonymisering av personuppgifter samt regelbunden testning och kvalitetsrevision av åtgärderna.
  - **De avtalsenliga villkoren för skydd av uppgifter** anges i avtalet mellan parterna.
- **Riskerna** i behandlingen ska beaktas vid bedömningen av lämpliga åtgärder.

Skydd av uppgifter – allmänt

- Handlingar eller filer som innehåller personuppgifter får inte behandlas på ett sådant sätt att utomstående kan se uppgifterna.
- I princip ska man undvika att ta utskrifter och kopior. Handlingar som innehåller personuppgifter får inte lämnas till vanlig pappersinsamling.
- Endast de som behöver personuppgifterna för att utföra sina arbetsuppgifter ska ha tillgång till uppgifterna.
- En behörighet som beviljats på grundval av arbetsuppgifter ska upphävas när uppgifterna för en anställd som företräder samarbetspartnern ändras eller personen lämnar organisationens tjänst.
- Datorn ska låsas varje gång man lämnar den.
- Efter användning av den elektroniska förbindelsen till förmånsdatatjänsten Kelmu ska förbindelsen stängas/ska man logga ut.
- Sekretessbelagda uppgifter eller personbeteckningar får inte skickas via okrypterad e-post.

Skydd av uppgifter – avtalsvillkor för skydd av uppgifter

1. Hos samarbetspartnern har en person utsetts till ansvarig för dataskydds- och datasäkerhetsärenden och FPA underrättas om dennes kontaktuppgifter.
2. Anvisningar ska meddelas om förfarandena för informationssäkerheten och de som använder den elektroniska förbindelsen för utlämnande av uppgifter ska bekanta sig med FPA:s utbildningsmaterial innan de använder förmånsdatasystemet Kelmu. Utöver utbildning av engångsnatur ska den utbildning och information som behövs skötas i behövliga intervaller.
3. Hanteringen av användarrättigheter ska vara ordnad med beaktande av datasäkerheten. Användarens användarrättighet ska godkännas av chefen eller någon annan som beviljar användarrättigheter. **Det väsentliga är att se till dels att åtkomsträttigheterna är nödvändiga för arbetsuppgifterna, dels att åtkomsträttigheterna upphävs när arbetsuppgifterna ändras eller anställningsförhållandet upphör.**
4. Samarbetspartnern ska införa förfaranden för övervakning av användningen av uppgifterna.
5. Uppgifternas konfidentialitet, integritet och tillgänglighet ska säkerställas så att den aktsamhets- och skyddsskyldighet som krävs enligt lagstiftningen fullgörs.
6. Kunderna informeras om användningen av (FPA:s) uppgifter.
7. Samarbetspartnerns personal ska informeras om följderna av felaktig behandling av personuppgifter.

Kela|Fpa

Personuppgiftsincidenter

Vad är en personuppgiftsincident?

- Med personuppgiftsincident avses en situation som leder till att personuppgifter förstörs, går förlorade, ändras, lämnas ut utan tillstånd eller görs tillgängliga för någon som inte bör ha tillgång till dem.
- Exempel:
  - att e-post skickas till fel adress
  - att handlingar hamnar på fel plats
  - att en dator stjäls eller försvinner
  - att ett USB-minne försvinner
  - hackning
  - infektion med skadeprogram
- De registrerades rättigheter äventyras till följd av en personuppgiftsincident.

Vad ska man göra vid en personuppgiftsincident?

- Rapportera omedelbart inom din organisation om en personuppgiftsincident som har eller som du misstänker har inträffat.
- Den personuppgiftsansvarige ska anmäla en personuppgiftsincident till
  - **tillsynsmyndigheten** utan onödigt dröjsmål och, om möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, och
  - **de registrerade** utan onödigt dröjsmål, om det är sannolikt att incidenten medför en hög risk för fysiska personers rättigheter och friheter.
- Tidsfristerna förlängs inte av veckoslut eller helger.
- Personuppgiftsincidenter ska alltid dokumenteras.

Kela|Fpa

Ansvar enligt dataskyddsförordningen

Typer av ansvar och skador

1. Ansvar för överträdelse av en administrativ förpliktelse (böter)
2. Skadeståndsansvar enligt lag för ekonomisk skada eller annan skada som orsakats en person
3. Ansvar på grund av avtalsbrott för (ekonomisk) skada som orsakats avtalsparten
4. Straffrättsligt ansvar

Administrativa påföljder

- Tillsynsmyndigheten kan meddela ett **förbud** som avbryter behandlingen av uppgifter.
- Tillsynsmyndigheten kan också ha rätt att påföra en **påföljdsavgift som grundar sig på hur allvarlig överträdelsen är.**
  - Böterna påförs av ett påföljdskollegium vid dataombudsmannens byrå.
  - Böternas storlek påverkas till exempel av de åtgärder som vidtagits för att begränsa skadan och av certifieringen av de egna processerna.
  - Enligt den nationella dataskyddslagen kan påföljdsavgifter **för närvarande inte påföras ett organ inom den offentliga förvaltningen**, men en ändring på denna punkt är under beredning och även i Finland kan en tjänsteleverantör som anlitas av den offentliga förvaltningen bli föremål för ändringen.
- Tillsynsmyndigheten har tillgång till ett brett utbud av medel.
  - Utöver behandlingsförbudet kan den exempelvis ge en anmärkning, begränsa behandlingen eller vidta motsvarande åtgärder.

Kela|Fpa

Laggrundat skadeståndsansvar för skada som orsakats den registrerade

- Om den personuppgiftsansvarige bryter mot dataskyddsförordningen och den registrerade därigenom orsakas materiell eller immateriell skada, har hen rätt till ersättning för skadan.
  - Materiell eller immateriell skada: både ekonomisk skada och eventuellt lidande ersätts.
- Skyddet gäller både de registrerade och andra **skadelidande**.
- Ersättningsansvaret för den arbetstagare eller tjänsteman som orsakat skadan kanaliseras i princip till den arbetsgivarorganisation som har rollen som personuppgiftsansvarig.

Skadeståndsskyldighetens dimensioner

- **Skadestånd till registrerade och betalning av påförda sanktioner till dataskyddsmyndigheten**
  - Grunden uppkommer enligt lag.
  - I praktiken kan det krävas flera års process vid allmänna domstolar.

- **Skadestånd enligt avtal i avtalsförhållande mellan två personuppgiftsansvariga**
  - Dataskyddsförordningen lägger grunden till en begränsad regressrätt i fråga om skadestånd som betalas till en registrerad för en avtalsparts räkning.
  - Ersättningsdimensionen bestäms av ett avtal mellan de personuppgiftsansvariga.

Den enskildes straffrättsliga ansvar

- Om personuppgifter behandlas obehörigt kan det leda till straffrättsligt ansvar för den enskilde.
- Behandling av personuppgifter som strider mot användningsändamålet eller de fastställda behörigheterna betraktas som spionerі för vilket ett personligt fängelsestraff kan dömas ut.

Sammandrag

Kom särskilt ihåg:

1. Det faktum att en viss uppgift existerar innebär inte att den får användas till vad som helst.
2. Se till att du förstår behovet av behandling: vad eftersträvas de facto med behandlingen och varför?
   - **Samarbetspartnern har rätt att med stöd av speciallagstiftningen få de nödvändiga uppgifter som den behöver för att sköta sina uppgifter.**
3. Om du är osäker, ta reda på och/eller tillämpa en tolkning som är förenlig med principerna för dataskydd.
4. Hanteringen av ansvar förutsätter att man identifierar skyldigheterna.
   - **Hanteringen av användarrättigheter är av avgörande betydelse. Det väsentliga är att se till dels att åtkomsträttigheterna är nödvändiga för arbetsuppgifterna, dels att åtkomsträttigheterna upphävs när arbetsuppgifterna ändras eller anställningsförhållandet upphör.**
5. För att uppgifterna ska kunna behandlas måste man utbilda sig och försäkra sig om sitt kunnande.

Kela|Fpa

Tack!

Kela|Fpa