Kompletterande anvisning för planering av hantering av data som innehåller känsliga och konfidentiella uppgifter 2019

Hänvisning: Arbetsgruppen ATT aineistonhallinnan ohje sensitiivisille aineistoille (2019) Anvisning för planering av hantering av data som innehåller känsliga och konfidentiella uppgifter, projektet Tuuli.
Zenodo: 10.5281/zenodo.3247282

CC 0 ZERO

Inledning	
	Denna anvisning gäller materialtyper som innehåller känsligt och konfidentiellt forskningsmaterial. Forskningsorganisationerna vägleder forskarna i tillämpningen av dataskydds- och datasäkerhetsprinciperna. Varje organisations allmänna anvisningar för datahanteringsplanen innehåller dessutom organisationens övriga centrala kontaktuppgifter för stödtjänster. Organisationerna kan också ha kombinerat denna anvisning och den allmänna anvisningen. Bekanta dig med din organisations datahanteringsanvisningar.
1. Allmän beskrivning av data	
1.1 Vilka typer av data baserar sig forskningen på? Hurdana data samlas in, skapas eller återanvänds? Vilka filformat används? Ge även en grov uppskattning av hur stor produktionen/insamlingen av data kommer att vara?	Specificera alla typer av data som innehåller personuppgifter, känsliga uppgifter eller konfidentiella uppgifter. Det är särskilt viktigt att identifiera känsliga delar av forskningsmaterialet, eftersom planeringen av datahanteringen fokuserar på att identifiera och hantera risker som är förknippade med dem. När det gäller personuppgifter ska du berätta vem som är *personuppgiftsansvarig.* Känslig och konfidentiell information är sådan som kan orsaka skada om den avslöjas: • Känsliga personuppgifter; det går inte att ge en heltäckande förteckning över känsliga personuppgifter. **De som utför en undersökning ansvarar för att identifiera sådana uppgifter som om de avslöjas kan ha skadeverkningar för de undersökta.** ○ Känsliga uppgifter kan gälla hälsa eller sjukdomsrisker, sexuell läggning, etniskt ursprung, medlemskap i fackförening och religiös övertygelse. • Sensitiva artdata, t.ex. uppgifter om utrotningshotade djur och växter, naturskydd eller biosäkerhet. • Annan konfidentiell information, t.ex. patent, landets försvar, organisatorisk information eller affärshemligheter.

	Tips Alla uppgifter på basis av vilka en person kan identifieras antingen *direkt* eller *indirekt* är personuppgifter. • *Direkta identifierare*: namn, telefonnummer, personbeteckning, foto, röstprov, fingeravtryck, tandkarta, MRI-bild • *Indirekta identifierare*: kön, ålder, utbildning, yrkesställning, nationalitet, lokaliseringsuppgifter, arbetshistoria, logguppgifter, civilstånd, bostadsort, en bils registernummer Länkar: Vad är en personuppgift (på finska och engelska (Finlands samhällsvetenskapliga dataarkiv FSD), Behandling av personuppgifter (Dataombudsmannens byrå)
1.2 Hur kontrolleras datamaterialets enhetlighet och kvalitet?	Fundera över hur eventuell minimering, pseudonymisering eller anonymisering påverkar datamaterialets kvalitet. https://www.fsd.uta.fi/aineistonhallinta/fi/tunnisteellisuus-ja-anonymisointi.html#milloin-tieto-on-anonyymia-enta-pseudonyymia https://tietosuoja.fi/sv/pseudonymiserade-och-anonymiserade-uppgifter
2. Iakttagande av etiska principer och lagsstiftning	
2.1 Vilka etiska frågor är relevanta för datahanteringen, t.ex. hantering av sensitiva data, skyddande av deltagarnas identitet, samtycke till delning av data?	Kontrollera *personuppgiftsansvaret* Behandling av särskilda kategorier av personuppgifter: https://tietosuoja.fi/sv/behandling-av-sarskilda-kategorier-av-personuppgifter • När får särskilda kategorier av personuppgifter behandlas? https://tietosuoja.fi/sv/behandling-av-sarskilda-kategorier-av-personuppgifter Dataombudsmannens byrå: Vanliga frågor https://tietosuoja.fi/sv/vanliga-fragor https://www.tenk.fi/fi/ihmistieteiden-eettinen-ennakkoarviointiohje-uudistuu (finskspråkig information om att anvisningarna om etikprövning inom humanvetenskaperna revideras) Nationell delegation TUKIJA: Nationella kommittén för medicinsk forskningsetik Kontrollera din organisations anvisningar.

2.2 Hur hanteras frågor som gäller äganderätten till datamaterialet, upphovsrätt och immateriella rättigheter? Finns det hinder för användningen eller delningen av data på grund av upphovsrätt, licenser eller andra begränsningar?	Avtal om äganderätten till datamaterialet och avtal om andra immateriella rättigheter ska alltid ingås innan de konkreta forskningsåtgärderna inleds. Det finns avtalsmallar och konsultation vid din egen forskningsorganisation.
3. Dokumentation och metadata	
3.1 På vilket sätt dokumenterar du ditt datamaterial så att det är sökbart, tillgängligt, interoperabelt och återanvändbart? Vilka metadatastandarder, README-filer eller annan dokumentation kommer att användas för att andra ska kunna förstå och använda datamaterialet?	När du beskriver datamaterialet bör du komma ihåg att även filnamn, filkatalognamn samt variabler och metadata kan innehålla personuppgifter eller känslig information. Du kan publicera metadata även om ditt forskningsmaterial innehåller personuppgifter, förutsatt att metadata inte innehåller information med identifierare som gör det möjligt att identifiera de undersökta personerna. • Making a research project understandable - Guide for data documentation DOI 10.5281/zenodo.1683181 • FSD:s handbok om datahantering (på finska och engelska)
4. Lagring och säkerhetskopiering under forskningsprojektet	
4.1 Var kommer datamaterialet att lagras och hur sker säkerhetskopieringen?	Enligt dataskyddsförordningen gäller det att bedöma riskerna med behandling av personuppgifter innan personuppgifterna börjar behandlas. Bekanta dig med din organisations dataskydds- och riskhanteringsanvisningar och fundera över följande: • Vilka friheter och rättigheter för den registrerade kan behandlingen äventyra? • Vilka skador kan den registrerade orsakas av den planerade behandlingen av personuppgifter? • Vilka skador kan den registrerade orsakas av att datamaterialet hamnar i fel händer, förstörs eller fördärvas? • Från vilka slags risker måste ditt datamaterial skyddas? • Med vilka medel kan identifierade risker hanteras? • Vad är en godtagbar nivå för sannolikheterna för och konsekvenserna av kvarstående risker? Efter bedömningen ska du kontakta dataskyddsombudet vid din organisation för att få bekräftat om ditt material kräver en konsekvensbedömning enligt dataskyddsförordningen. Utred också om externa aktörer, t.ex. forskningsfinansiären eller ägaren till datamaterialet, har egna krav som gäller materialet.

	Utgående från riskbedömningen fastställs skyddsåtgärder för materialets hela livscykel. (Se även punkt **4.2**.)
	
	Fundera över följande:
	
	• Vilka lagringstjänster och lagringsenheter används under forskningsprojektets gång?
	• Vem ansvarar för driften av de lagringstjänster som används?
	• Hur utförs säkerhetskopieringen i de lagringstjänster som du använder?
	  o Vem ansvarar för säkerhetskopieringen?
	  o Var lagras säkerhetskopiorna?
	  o Hur ofta tas säkerhetskopior?
	  o Hur länge bevaras säkerhetskopiorna?
	• För lagringstjänsterna bok (logg) över hur materialet används?
	• Kan materialet användas på distans?
	  o Om svaret är ja, hur skyddas distansanvändningen?
	• Behöver uppgifterna krypteras?
	  o Om svaret är ja, fundera över följande:
	  ▪ Vilken del av materialet krypteras och vilken del krypteras inte?
	  ▪ Vilka krypteringsverktyg används?
	  ▪ Vem administrerar krypteringsnycklarna och lösenorden?
	• Hur har de lokaler som används för att behandla datamaterialet skyddats?
	  o Går det att låsa dörrarna till arbetslokalerna?
	  o Känner du alla personer med tillträde?
	  o Finns det kamerabevakning med inspelning i fastigheten?
	  o Finns det inbrottssäkra förvaringsmöbler eller förvaringsutrymmen för fysiska datamaterial och lagringsenheter?
	  o Är arbetsborden (arbetsplatserna) skyddade mot insyn?
	• Hur utplånas datamaterialet och kopiorna på ett tryggt sätt när de inte längre behövs?
	
	Bekanta dig med din organisations anvisningar om lagringstjänster och verktyg som garanterar att data behandlas på ett datasäkert sätt. Ta också reda på serviceadressen till din organisations datasäkerhetsenhet och it-enhet.
	
	Ytterligare information:

	Riskbedömning (Dataombudsmannens byrå) Konsekvensbedömning (Dataombudsmannens byrå)

4.2 Vem reglerar åtkomsten till datamaterialet och hur övervakas skyddad åtkomst?	Åtkomsten till personuppgifter ska begränsas så att endast de som behöver personuppgifterna för att utföra undersökningen har åtkomst till dem. Kom ihåg att denna persongrupp omfattar även de som ansvarar för de tjänster och verktyg som du använder samt andra, eventuellt externa tjänsteleverantörer.
	
	Fundera över följande:
	
	• Hur, av vem och på vilket sätt behöver datamaterialet kunna användas?
	  ○ Vem kan beviljas användningsrätt?
	  ○ Hurdan användning är tillåten?
	  ○ Vilka slags användarrättigheter krävs för olika delar av materialet?
	  ○ Behöver data delas med samarbetspartner eller tjänsteleverantörer?
	  ○ Vem kan överföra data från en part till en annan och på vilka grunder?
	• Hur övervakas användning och tillträde?
	  ○ Vem ansvarar för åtkomsträttigheterna?
	  ○ Är användar- och tillträdesrättigheterna dokumenterade och kan de modifieras och raderas?
	  ○ Kontrolleras rättigheternas grund och avgränsning regelbundet?
	• Hur övervakas användningen av datamaterialet och att användningen är tillbörlig?
	  ○ Hur ofta kontrolleras användarrättigheterna?
	  ○ Vart och för vem kopieras datamaterialet eller delar av det?
	  ○ Hur hanteras kopior av materialet?
	  ○ Hur raderas kopiorna när användningsrätten upphör?
	  ○ Hur försäkrar man sig om användningsändamålen?
	• Har de som behandlar datamaterialet uppdaterad dataskydds- och datasäkerhetskompetens och uppdaterade anvisningar om behandlingen?
	
	Bekanta dig med din organisations principer, anvisningar och verktyg för hantering av åtkomsträttigheter. Utred hur man vid din organisation rapporterar om missbruk och skador relaterade till personuppgifter.

5. Öppna, publicera och arkivera data efter avslutat forskningsprojekt	

5.1 Vilken del av datamaterialet kan göras öppet tillgängligt eller publiceras? Var och när kommer datamaterialet eller dess metadata att göras tillgängliga?	Datamaterial som innehåller personuppgifter kan endast göras öppet tillgängligt i anonymiserad form. Det lönar sig också annars att anonymisera eftersom anonymiserade data inte längre är personuppgifter, vilket innebär att de inte omfattas av dataskyddslagstiftningen och att det är möjligt att göra dem öppet tillgängliga och att dela dem. Pseudonymiserade data är fortfarande personuppgifter och kan därför inte göras öppet tillgängliga. Data som innehåller personuppgifter kan dock med separat tillstånd delas med intresserade för ändamål i överensstämmelse med den ursprungliga behandlingsgrunden. Den ursprungliga grunden för behandling av datamaterial som innehåller personuppgifter, exempelvis en lagbaserad grund eller ett samtycke, kan begränsa framtida användning av materialet. Om exempelvis den ursprungliga blanketten för samtycke inte har noterat möjligheten att återanvända datamaterialet, kan det krävas ett nytt samtycke av den undersökta personen för att materialet ska kunna öppnas. Datamaterial som innehåller personuppgifter kan öppnas eller publiceras på följande sätt: 1. Data anonymiseras och anonymiserade data öppnas i ett dataarkiv. 2. Centrala metadata publiceras (i ett forskningsdatasystem eller i någon annan publiceringstjänst) och det egentliga datamaterialet ställs till förfogande med tillstånd från den som producerat det eller från ett tillförlitligt datarepositorium. *Länkar* • Pseudonymiserade och anonymiserade uppgifter: https://tietosuoja.fi/sv/pseudonymiserade-och-anonymiserade-uppgifter • Identifierare och anonymisering (på finska): http://www.fsd.uta.fi/aineistonhallinta/fi/tunnisteellisuus-ja-anonymisointi.html • Etsin, publiceringstjänst för metadata (på finska och engelska): https://etsin.fairdata.fi/
5.2 Var bevaras datamaterial av långsiktigt värde och hur länge?	Undervisnings- och kulturministeriet erbjuder högskolorna och forskningsinstituten en tjänst för långtidsbevaring av forskningsdata (den s.k. PAS-tjänsten). Varje organisation bestämmer sin process för att identifiera forskningsdata av långsiktigt värde och för att överföra datamaterialet till PAS-tjänsten. Beroende på organisationens

	anvisningar och forskningstillståndet är det möjligt att i PAS-tjänsten lagra även datamaterial som innehåller känsliga personuppgifter. För arkivering av datamaterial som innehåller känsliga personuppgifter krävs bevaringstillstånd av Nationalarkivet, och materialet måste minimeras före arkiveringen. Data som bevarats på detta sätt kan återanvändas med forskningstillstånd. I regel rekommenderas det att känsligt material utplånas efter forskningsprojektet, eftersom bevaringen medför risker och kräver specialarrangemang. Därför är det viktigt att också planera hur data ska utplånas på ett säkert sätt. Det räcker exempelvis inte nödvändigtvis med att radera (delete) filerna och tömma datorns papperskorg för att de ska förstöras slutgiltigt. Det går att återskapa borttagna data till och med efter att hårddisken har initierats på nytt. Det finns olika typer av programvara för slutgiltig utplåning av data, och de fungerar exempelvis så att de skriver över data eller magnetiserar hårddisken. Du kan också förstöra lagringsenheten mekaniskt t.ex. genom att krossa den. Anonymisering leder till att datamaterialet inte längre innehåller personuppgifter och följaktligen inte omfattas av dataskyddslagstiftningen. *Tips* • Kom ihåg att du måste se till att datamaterialet anonymiseras och utplånas eller arkiveras inom den utsatta tiden för forskningstillståndet. • Äkta anonymisering förutsätter att möjligheterna till såväl direkt som indirekt identifiering elimineras och att identifieringsnyckeln förstörs. • Många högskolor och forskningsinstitut har interna anvisningar för utplåning av lagringsverktyg. *Länkar* • Utplåning av forskningsmaterial (på finska): http://www.fsd.uta.fi/aineistonhallinta/fi/fyysinen-sailytys.html#havittaminen
6. Datahanteringens ansvar och resurser	
6.1 Vem ansvarar för specifika uppgifter i datahanteringen under projektets livscykel? Uppskatta även de resurser	Vem **ansvarar** för hanteringen av känsligt och konfidentiellt datamaterial och för tillsynen över hanteringen under materialets hela livscykel?

som krävs för datahantering (t.ex. finansiering, tid och arbetsmängd).	• Vem ansvarar för *dataskyddet* (se punkt 2) och *datasäkerheten* (se punkt 4)? Vid planeringen av behövliga **resurser** gäller det att beakta • kostnaderna för minimering, pseudonymisering och anonymisering, dvs. hur mycket tid och vilken programvara som behövs • kraven på att verksamheten och tekniken når upp till en högre säkerhetsnivå samt merkostnaderna för dessa.