Framgangsmåte for risikovurdering av forskningsprosjekter

Beskriv den planlagte dataflyten i prosjektet. Gå gjennom og beskriv hendelser og situasjoner som kan føre til at personopplysninger kommer på avveie, går tapt eller blir utilgjengelige for de som skal ha tilgang i alle faser av datahåndteringen (innsamling, overføring, lagring, behandling/analyse, eventuell deling, avslutning). Aktuelle tema kan være hendelser knyttet til overføring av data, utskrift, tilgangskontroll og kontroll på fysisk utstyr. Det er allerede fylt inn noen eksempler på hva som kan gå galt, tilpass disse til prosjektet og legg til nye.

Hovedfokus skal være på mulige konsekvenser for de registrerte (tap av anseelse/integritet dersom opplysninger som oppleves som følsomme eller som kan misbrukes, kommer på avveie), men konsekvensene for institusjonen (økonomisk tap, økonomiske sanksjoner, tap av omdømme) skal også tas med i betraktning. Husk at konsekvensen (og dermed risikoen) som regel er større for særlige kategorier enn for alminnelige personopplysninger.

Gå deretter gjennom hvilke eventuelle tiltak som allerede eksisterer, og hvilke tiltak som kan settes inn for å redusere risikoen (sannsynlighet og/eller konsekvens) ytterligere.

I mange tilfeller vil konsekvensen av brudd på personopplysningssikkerheten ikke la seg redusere. Det vil likevel som regel gå an å redusere sannsynligheten.

I noen tilfeller vil det ikke la seg gjøre å få sannsynligheten ned til grønt. Noe restrisiko må som regel aksepteres, og det er opp til hvert enkelt prosjekt (eventuelt institutt, dersom det er mye restrisiko) å avgjøre hvor mye risiko prosjektet kan håndtere.

Risikonivå	I disse kolonnene noteres tallverdier for sannsynlighet og konsekvens/skade. Dette gjøres for hver enkelt uønsket hendelse som er notert i regnearket. Sannsynligheten varierer fra svært lite sannsynlig (tallverdien 1) til svært sannsynlig (tallverdien 4). Konsekvensen/skaden varierer fra lite alvorlig (tallverdien 1) til svært alvorlig (tallverdien 4).
Konsekvens	
1	Lite alvorlig. Har ubetydelige skadevirkninger for enkeltpersoner eller institusjonen.
2	Mindre alvorlig. Har visse skadevirkninger for enkeltpersoner eller institusjonen. Eksempel: Uautorisert eksponering av noen få alminnelige personopplysninger
3	Alvorlig. Har merkbare skadevirkninger for enkeltpersoner eller institusjonen. Eksempel: Uautorisert eksponering av fortrolige/sensitive eller større mengder alminnelige personopplysninger.
4	Svært alvorlig. Har store skadevirkninger for enkeltpersoner eller institusjonen. Eksempel: Uautorisert eksponering av større mengder sensitive personopplysninger.

Sannsynlighet	
1	Svært lite sannsynlig - vil mest sannsynlig ikke skje i løpet av prosjektperioden
2	Lite sannsynlig - kan forekomme i løpet av prosjektperioden.
3	Sannsynlig - vil sannsynligvis skje i løpet av prosjektperioden.
4	Svært sannsynlig - kan potensielt skje flere ganger i løpet av prosjektperioden.
Risikoverdi	
Rød (8-16)	Hendelser med høy risiko. Nye tiltak skal innføres.
Gul (4-7)	Hendelser med moderat risiko. Nye tiltak bør vurderes.
Grønn (1-3)	Hendelser med lav risiko.
Tiltak	List opp aktuelle organisatoriske, menneskelige og teknologiske tiltak som kan redusere sannsynlighet og/eller konsekvens.
	Eksempler på organisatoriske tiltak: Utforming av retningslinjer, avviksrutiner, organisering av tilganger, internkontroll etc.
	Eksempler på menneskelige tiltak: Opplæring, bevisstgjøring av brukere, endring av praksis etc.
	Eksempler på teknologiske tiltak: Tofaktorautentisering, kryptering, tilgangskontroll etc.
	(innebærer ofte valg av NTNU-godkjente løsninger for innsamling, overføring og lagring)