Vejledning om risikovurdering og metode

Organisation	**Databeskyttelsesrådgiverfunktion i Den Storkøbenhavnske Digitaliseringsforening (DSD)**
Dokument navn	Vejledning om risikovurdering og metode v1.0.docx
Dokument ejer	Daniel Bach, Michael Drews Olsen
Senest ændret	5. april 2019
ISO 27001 reference	8.2 – Vurdering af informationssikkerhed
GDPR reference	Artikel 32 – Gennemførelse af passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et passende sikkerhedsniveau.

Version	Dato	Revisions forfatter	Beskrivelse
1.0	5. april 2019	Daniel Bach	Første version

Formål: Formålet med denne vejledning er at hjælpe kommunerne med risikovurdering og gennemførelse af passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et passende sikkerhedsniveau for de behandlede personoplysninger, jf. artikel 32, i persondataforordningen.

Omfang: Alle kommuner tilsluttet DSD's fælles databeskyttelsesrådgiverfunktion.

Indhold

Et hovedformål efter forordningen

Det er et af persondataforordningens hovedformål at sikre beskyttelse af behandlede personoplysninger. Forordningen foreskriver, at der skal gennemføres *passende* tekniske og organisatoriske foranstaltninger, som sikrer et sikkerhedsniveau, der passer til risikoen forbundet med behandlingen af personoplysninger, jf. artikel 32 i forordningen.

Afvejning af risiko og sikkerhedsforanstaltninger

Forordningen lægger med andre ord op til, at der i forbindelse med vurderingen af, hvad der er et passende sikkerhedsniveau, skal foretages en afvejning, hvor risikoen udgør vægtloddet i den ene vægtskål, og hvor sikkerhedsforanstaltninger udgør vægtloddet i den anden vægtskål.

Det første led i afvejningen består i at identificere risikoen på baggrund af en risikovurdering. Det andet led i afvejningen udgøres af de sikkerhedsforanstaltninger, der - på baggrund af risikovurderingen - gennemføres for at sikre et passende sikkerhedsniveau. Hvad der er passende sikkerhedsforanstaltninger, beror således på den foretagne risikovurdering.

Grundlaget for risikovurdering

Det er et krav efter forordningens artikel 32, stk. 1, at der gennemføres sikkerhedsforanstaltninger under hensyntagen til:

- Aktuelt teknisk niveau
- Implementeringsomkostninger
- Den pågældende behandlings karakter, omfang, sammenhæng samt formål
- Risici af varierende sandsynlighed for de registreredes rettigheder og frihedsrettigheder

Den pågældende behandlings karakter

Der skal tages højde for behandlingens karakter, fordi der er højere risiko ved at behandle følsomme personoplysninger end almindelige personoplysninger. Men det er ikke nok kun at sondre mellem følsomme og almindelige personoplysninger, fordi der også er forskel på risiko forbundet med behandling af almindelige personoplysninger. Der er højere risiko ved at behandle tavshedsbelagte personoplysninger (f.eks. væsentlige sociale problemer) om de registrerede end almindelige

personoplysninger om f.eks. alder og fødselsdato. Der er også højere risiko ved at behandle personoplysninger om børn end om voksne, fordi børn nyder en særlig beskyttelse efter forordningen.

Den pågældende behandlings omfang
Der skal tages hensyn til behandlingens omfanget. Dette gælder både, hvor der er tale om flere data om de samme registrerede, og hvor der er tale om mange registrerede. Der er som regel en større risiko ved behandling af personoplysninger et stort antal registrerede end få registrerede. Der er på samme vis som regel større risiko ved behandling af mange forskellige typer af oplysninger om de registrerede end behandling af nogle få datatyper om det samme antal registrerede.

Den pågældende behandlings sammenhæng
Den sammenhæng, som oplysningerne behandles i, skal der også tages højde for i risikovurderingen. Selvom en oplysning isoleret set ikke udgør en høj risiko, vil den sammenhæng, som oplysningen behandles i, kunne medføre, at risikoen forhøjes. F.eks. vil en almindelig personoplysning om navn og adresse i et medlemsregister medføre en højere risiko, hvor der er tale om en politisk eller religiøs forening, end hvis der er tale om en sportsforening.

Formålet
Der skal tages hensyn til formålet med behandlingen. Risikoen for de registrerede er ikke kun et spørgsmål om uberettiget adgang til personoplysninger, men også manglende tilgængelighed til personoplysninger. Hvis formålet med behandlingen af personoplysninger f.eks. er at yde sundhedsydelser til de registrerede, kan manglende adgang til oplysningerne i kommunen have alvorlige helbredsmæssige konsekvenser for den registrerede.

Det følger af forordningens artikel 32, stk. 2, at der ved vurderingen af, hvilket sikkerhedsniveau, der er passende, navnlig tages hensyn til de risici, som en behandling udgør ved:

- Hændelig eller ulovlig tilintetgørelse, tab eller ændring
- Uautoriseret videregivelse af personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
- Uautoriseret adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

Kravene i forordningens artikel 32, stk. 1-2, vil blive inddraget i gennemgangen af metode (se nedenfor)

Metode

Forordningen angiver ikke metode for risikovurdering, men det er et krav, at risiko evalueres på grundlag af en objektiv vurdering, som gør det muligt at fastslå den risiko, behandlingen af personoplysninger indebærer. Det betyder, at kommunen skal risikovurdere efter en beskrevet og defineret metode. Kommunen skal dokumentere metoden, fordi kommunen skal kunne påvise, at der er foretaget en risikovurdering i overensstemmelse med forordningens artikel 32.

Der kan hentes inspiration i metoder for risikovurdering i sikkerhedsstandstandarder, men risikovurderingen skal tage højde for de krav, som følger af artikel 32, stk. 1-2.

I det følgende gennemgås metode, som er inspireret af sikkerhedsstandarden ISO 27005, men hvor der tages højde for de krav til risikovurdering, som følger af forordningen.

Kommunen kan anvende følgende risikometode: *Sandsynlighed gange konsekvens = risiko*

Processen for risikovurdering kan deles op i følgende trin:

1. Etablering af kontekst
2. Risikoidentifikation
3. Risikovurdering
4. Risikoevaluering
5. Risikohåndtering

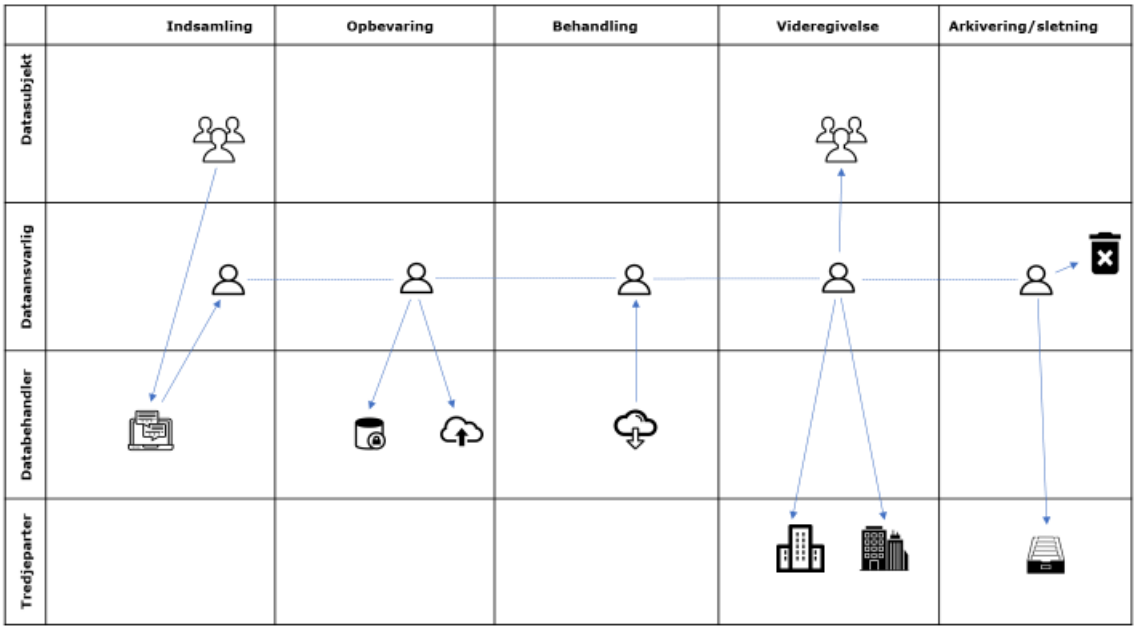
1. Etablering af kontekst

På det første trin skal det defineres nærmere, hvad der er genstanden for risikovurderingen (f.eks. behandlingsaktiviteter, dataprocesser og it-systemer). Understøttende aktiver (f.eks. programmer, systemer og netværk) til det, som skal risikovurderes, bør også beskrives.

Det er allerede i forbindelse med etableringen af konteksten en god ide at beskrive, hvilke personoplysninger der indgår i behandlingen, den sammenhæng, de behandlede personoplysninger indgår i, formålet med den behandling, som udføres eller påtænkes udført, herunder mængden af personoplysninger og antal registrerede, fordi dette har betydning for risiko og i henhold til artikel 32, stk. 1, i forordningen, skal inddrages i forbindelse med vurdering af sandsynlighed og konsekvens.

Der bør udpeges medarbejdere og defineres roller for de medarbejdere, som skal deltage i risikovurderingen (f.eks. sikkerhedskoordinator, it-teknikere, fagansvarlige og/eller fagrepræsentanter).

Et overblik over personoplysninger i et dataflow diagram vil gøre det nemmere at overskue konteksten, som skal risikovurderes. Et dataflow diagram bør afspejle personoplysningerne i hele livscyklussen; fra indsamling til arkivering og sletning. Eksempel på dataflow diagram:



2. Risikoidentifikation

På dette trin skal relevante trusler og sårbarheder identificeres med henblik på at kunne vurdere sandsynlighed og konsekvenser. En trussel vil normalt være irrelevant, hvis der ikke findes en sårbarhed, hvori truslen kan udmønte sig.

Der kan hentes inspiration i trusselskataloger, hvorfra der kan udvælges trusler, som er relevante[1]. Trusler bør udvælges fra kataloger eller defineres af kommunen på baggrund af historik/statistik for hændelser i kommunen eller fra hændelser i andre offentlige myndigheder eller private virksomheder. Sårbarheder kan bl.a. identificeres inden for følgende områder: hardware, software, netværk, personale, websted og organisering. Der kan f.eks. hentes inspiration i kataloger om sårbarheder i sikkerhedsstandarder[2].

De identificerede trusler og sårbarheder kan oplistes i et skema for risikovurdering, som kan anvendes som værktøj for risikovurderingen. I skemaet kan der oprettes rækker til beskrivelse af hændelse for hver enkelt trussel, vurdering af sandsynlighed og score, vurdering af konsekvenser og score, herunder række for samlet risikoscore for hver trussel.

Se bilag 1 for eksempel på skema for risikovurdering.

3. Risikoanalyse

På dette trin skal sandsynlighed og konsekvens vurderes.

Vurdering af sandsynlighed

Sandsynlighed findes ved at vurdere, hvor stor sandsynlighed der er for, at en trussel indtræder under hensyntagen til de identificerede sårbarheder. Vurderingen foretages under inddragelse af historisk/statistisk grundlag for sikkerhedsbrud eller brud på persondatasikkerhed i kommunen, hvis dette forefindes.

I vurderingen af sandsynlighed skal der, jf. artikel 32, stk. 1, tages højde for, om den pågældende behandlings karakter, omfang, sammenhæng samt formål har betydning for truslens sandsynlighed. Vurderingen af sandsynlighed kan med fordel foretages ved brug af en egnet sandsynlighedsskala, som sikrer en objektiv vurdering af sandsynlighed og score (se eksempel på en sådan nedenfor).

Eksempel på sandsynlighedsskala:

Sandsynligheds-skala	Eksempel beskrivelse
1. Usand-synligt	Det anses for næste udelukket, at hændelsen nogensinde kan forekomme • Ingen erfaring med hændelsen • Kendes kun fra få andre offentlige eller private virksomheder

[1] European Union Agency for Network and Information Security (ENISA) har udarbejdet et trusselskatalog, der kan findes her: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

The German Federal Office for Information Security (BSI) har også udarbejdet trusselskataloget – grundlæggende trusler, der kan findes her: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf?__blob=publicationFile&v=2]

ISO 27002, anneks C, og ISO 29134, anneks B indeholder trusselskataloger.

[2] ISO 27005, anneks D.

2. Mindre sandsynligt	Hændelsen forventes ikke at indtræde • Ingen erfaring med hændelsen • Hændelsen kendes kun fra få andre offentlige eller private virksomheder, men ikke i Danmark
3. Sandsynligt	Det er sandsynligt at hændelsen vil forekomme • Kommunen har erfaring med hændelsen, men ikke inden for de sidste 12 måneder • Kendes fra andre offentlige eller private virksomheder i Danmark (hændelsen omtales ofte i pressen eller på offentlige hjemmesider)
4. Forventet	Det ventes at hændelsen vil forekomme • Man har erfaring med hændelsen inden for de sidste 12 måneder • Hænder jævnligt i andre offentlige myndigheder eller private virksomheder (omtales ofte i pressen eller på offentlige hjemmesider)

Praktisk fremgangsmåde
Vurderingen af sandsynlighed, som foretages i forhold til hver enkelt trussel, kan kort begrundes i relevant felt i skema for risikovurdering eller i et andet dokument eller værktøj, som er egnet til brug for risikovurderingen. I det omfang, der er lagt vægt på historisk/statistisk grundlag for vurderingen af sandsynlighed, bør dette også kort begrundes. Der vælges et niveau fra en sandsynlighedsskala, som matcher til den vurderede sandsynlighed. Score angives i relevant felt i skema for risikovurdering eller i et andet dokument eller værktøj til brug for risikovurderingen.

Se bilag 1 for eksempel på vurdering af sandsynlighed.

Vurdering af konsekvens
Konsekvens findes ved at vurdere, hvad der er konsekvensen for de registrerede, hvis en trussel indtræder. Der skal, jf. artikel 32, stk. 2, ses på, hvilken konsekvens det har for de registrerede, hvis:

- personoplysninger om de registrerede hændeligt eller ulovligt tilintetgøres, fortabes eller ændres
- uvedkommende får kendskab eller adgang til personoplysninger om de registrerede
- manglende adgang til registreredes personoplysninger

De situationer, som der skal ses på efter artikel 32, stk. 2, er omfattet af parametrene:

- tab af fortrolighed,
- tab af integritet og
- tab af tilgængelighed

Fortrolighed, integritet, tilgængelighed og robusthed er parametre, der dækker over en grundlæggende tilgang til sikkerhed. "Fortrolighed" dækker over, at der ikke må være uautoriserede adgang til eller anvendelse af personoplysninger eller af det udstyr, der anvendes til behandlingen. Med udtrykket "integritet" sigtes bl.a. til, at det skal være muligt at validere, om oplysninger på systemer er korrekte. For så vidt angår begrebet "tilgængelighed" sigtes bl.a. til at behandlingssystemer og -tjenester og oplysninger i disse konstant er tilgængelige ved anmodning fra autoriseret bruger

Ved vurderingen af konsekvenser for de registrerede tages der udgangspunkt i parametrene nævnt ovenfor. Der skal således foretages en vurdering af konsekvenserne for de registrerede separat for tab af fortrolighed, integritet og tilgængelighed. Vurderingen skal, jf. præambel 76 til forordningen, tage højde for følgende konsekvenser for de registrerede ved tab af fortrolighed, integritet og tilgængelighed:

- Fysisk skade
- materiale skade
- moralsk skade

- Forskelsbehandling
- Identitetstyveri
- Identitetssvig
- Økonomiske konsekvenser, herunder finansielle tab
- Skade på omdømme
- Indflydelse på privatliv
- Skade på omdømme
- Sociale konsekvenser
- Indflydelse på privatliv
- Skade på menneskelig værdighed
- Skade på legitime interesser
- Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder
- Forhindring i udøvelse af kontrol med egne personoplysninger

Der skal også tages højde for, om den pågældende behandlings karakter, omfang, sammenhæng, herunder formål, har betydning for konsekvens, jf. artikel 32, stk. 1. Det skal således afspejles i vurderingen af konsekvens, om der er tale om følsomme eller almindelige personoplysninger, herunder om der er tale om tavshedsbelagte personoplysninger, om der er er tale om stort omfang personoplysninger og/eller antal registrerede, sammenhængen, som oplysningernes behandles i, herunder formål med behandlingen.

Kommunen skal herudover tage højde for, hvor stor skaden ved, at truslen indtræder, er for de registrerede.

Vurderingen af konsekvenser for de registrerede, og hvor stor skaden er for de registrerede, kan med fordel foretages ved brug af en egnet skala for konsekvensniveauer, som tager højde for kravene efter forordningen (se straks eksempel på sådan en skala nedenfor).

Eksempel på skala for konsekvensniveauer:

Konsekvensniveau	Eksempel beskrivelse
1. Lav	De registrerede kan opleve få uhensigtsmæssigheder, de kan overkommes og imødegås uden større indsats (f.eks. tid på genindtastning af oplysninger, dårlig oplevelse, gener, irritationer og lign.).
2. Middel	De registrerede kan opleve betydelige uhensigtsmæssigheder, som de kan overvinde med en indsats og overvindelse af nogle få besværligheder (ekstra omkostninger, manglende adgang til services eller betjening, frygt, manglende forståelse, stress og mindre påvirkning af fysisk karakter og lign.)
3. Høj	De registrerede kan opleve betydelige konsekvenser, som kun kan overkommes med en betydelig indsats og konsekvenser for den enkelte (økonomiske konsekvenser, herunder finansielle tab, fejlkontering af midler, sortlistning elle nedgradering i kreditmuligheder, fysisk skade på aktiver, påvirkning af arbejdssituation, dårligere helbred og påvirkning af menneskelig værdighed og omdømme og lign.
4. Meget høj	De registrerede kan opleve betydelige og indgribende konsekvenser, som det ikke er muligt eller kun vanskeligt muligt at overkomme (mistet erhvervsevne, langvarige fysiske og psykiske påvirkninger, tab af fundamentale rettigheder, død og lign.)

Praktisk fremgangsmåde
Vurderingen af konsekvenser, som foretages separat for tab af fortrolighed, integritet og tilgængelighed i forhold til hver enkelt trussel, kan kort begrundes i felt i skema for risikovurdering eller i et andet dokument eller værktøj, som er egnet til brug for risikovurderingen.

I det omfang, det er vurderet, at den pågældende behandlings karakter, omfang, sammenhæng samt formål, jf. artikel 32, stk. 1, har betydning for konsekvens, bør dette kort begrundes. Der vælges niveau fra skala for konsekvensniveauer, som matcher til de vurderede konsekvenser. Score indsættes i relevante felter i skemaet for risikovurdering eller i andet dokument eller værktøj til brug for risikovurderingen.

Se bilag 1 for eksempel på vurdering af konsekvens.

4. Risikoevaluering

På dette trin skal der findes risikoscore for hver enkelt trussel på baggrund af risikovurderingen. Risikoscoren findes på baggrund af risikometoden: sandsynlighed (trussel + sårbarhed) gange konsekvens (ved tab af fortrolighed, integritet og tilgængelighed) = risiko.

Konsekvenser for de registrerede bør beregnes ved at anvende det højeste konsekvensniveau fra de tre separate vurderinger af konsekvenser for de registrerede ved tab af fortrolighed, integritet og tilgængelighed[3]. På denne måde opnås et risikobillede for de registrerede, hvor der tages højde for worst case scenarier for konsekvenserne for de registrerede. I beregningen ganges det højeste konsekvensniveau med sandsynlighed, hvormed der opnås en risikoscore for hver enkelt trussel.

Resultaterne fra risikoevalueringen kan indsættes i skema for risikovurdering eller i særskilt skema, hvor risiko kan rankes. Eksempel på særskilt skema:

Trussel	**Sandsynlighed**	**Konsekvens**			**Risikoscore**	**Rank ***
		Fortrolighed	Integritet	Tilgængelighed		
1.1 Tab af pc'er under transport fra eller til arbejde	3	3	2	2	**9**	**2**
	Risiko	**9**	**6**	**6**		
1.2 Tab af USB-stik mellem dataindsamling	4	3	3	3	**12**	**1**
	Risiko	**12**	**12**	**12**		

For at skabe et overblik for risikoniveauerne til brug for risikohåndteringen (se afsnittet nedenfor) kan der udarbejdes en risikoratio og risikomatrix, hvor hver enkelt trussel kan plottes ind i matrixen alt efter truslens risikoscore.

Eksempel på risikoratio:

Risikoratio	**Risikoniveau**	**prioritering**
1-4	Lav	
5-8	Middel	
9-12	Høj	
13-16	Meget høj	

[3] Se ENISA Guidelines for SMS's on the security of personal data processing, pkt. 3.2.3, side 22-23, som kan findes her: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

Eksempel på risikomatrix, hvor trusler er plottet ind:

Sandsynlighed →

Konsekvens ↓

	Usandsynligt	Mindre sandsynligt	Sandsynligt	Forventet
Lav	1	2	3	4
Middel	2	4	6	8
Høj	3	6	9 (1.1)	12 (1.2)
Meget høj	4	8	12	16

5. Risikohåndtering

På det sidste trin skal der gennemføres passende tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af risikovurderingen. Hvad der er *passende* sikkerhedsforanstaltninger, beror som tidligere nævnt på risikoen. Det betyder, at kommunen skal forholde sig til risikoscoren for hver enkelt trussel i forbindelse med vurderingen af, hvilke sikkerhedsforanstaltninger der skal gennemføres.

Det følger af forordningens artikel 32, stk. 2, at der bør overvejes følgende forhold, når det skal besluttes, hvilke foranstaltninger der skal gennemføres for at sikre et passende sikkerhedsniveau:

- Brug af pseudonymisering og kryptering
- Sikring af fortrolighed og integritet
- Systemers tilgængelighed og modstandsdygtighed (robusthed)
- Muligheden for at genskabe tilgængelighed og adgang til de behandle personoplysninger inden rimelig tid
- Processer, der sikrer, at der sker løbende afprøvning og vurdering af de gennemførte sikkerhedsforanstaltningers effektivitet

Sikkerhedsforanstaltningerne, som er nævnt ovenfor, er ofte relevante for at sikre en beskyttelse af personoplysninger, men kommunen skal altid foretage en konkret vurdering af, hvilke foranstaltninger der sikrer et passende sikkerhedsniveau.

Kommunen skal i den forbindelse være opmærksom på, at det er ikke tilstrækkeligt kun at gennemføre tekniske sikkerhedsforanstaltninger, fordi det følger af forordningen, at der også skal gennemføres organisatoriske foranstaltninger. Organisatoriske foranstaltninger kan f.eks. være uddannelse af medarbejdere, fordeling af roller og ansvar samt adgangsstyring til personoplysninger og systemer.

Kommunen kan overveje at bruge sikkerhedsforanstaltninger fra sikkerhedsstandarder, f.eks. ISO 27002. Det er dog vigtigt, at kommunen ikke bruger standarder som en sovepude, men gennemfører foranstaltningerne på baggrund af en konkret vurdering af risiko.

I vurderingen af, hvilke sikkerhedsforanstaltninger der skal gennemføres, skal der efter artikel 32, stk. 1, tages hensyn til:

- det aktuelle tekniske niveau og
- implementeringsomkostninger

Det aktuelle tekniske niveau og implementeringsomkostninger
Begrebet det aktuelle tekniske niveau dækker over, hvilke tekniske muligheder for beskyttelse af personoplysninger, der er tilgængelige for kommunen og/eller databehandler, men også på markedet. Kommunen skal således tages hensyn til, hvilke muligheder der er tilgængelige i forbindelse med vurderingen af, hvilke sikkerhedsforanstaltninger der skal implementeres.

Kommunen skal også tages hensyn til omkostningerne forbundet med implementeringen. Der er således ikke et krav om, at kommunen altid skal implementeres de nyeste, og forventeligt dyreste, sikkerhedsforanstaltninger for beskyttelse af personoplysninger. Kommunen kan dog ikke anvende omkostningerne som en undskyldning for ikke at yde tilstrækkelig sikkerhed for de behandle personoplysninger. Hensynet er derimod en ventil, som sikrer, at der ikke stilles krav om meget dyre sikkerhedsforanstaltninger, hvis dette kun giver en marginalt bedre sikkerhed. Kommunen skal således have et vist kendskab til de tilgængelige muligheder, og vurdere, om det kan svare sig at investere i disse, eller om andre billigere foranstaltninger kan give samme eller næsten samme beskyttelse.

Praktisk fremgangsmåde
De gennemførte sikkerhedsforanstaltninger på baggrund af risikovurderingen dokumenteres i et risikoregister eller andet værktøj, som er egnet til håndtering af risiko. I det omfang, der er tilbageværende høj risiko, der indebærer, at der ikke er et passende sikkerhedsniveau for personoplysningerne, skal dette dokumenteres med henblik på afhjælpning. Det bør i den forbindelse dokumenteres, hvem der er ansvarlig for afhjælpning og planlagt tidspunkt for afhjælpning, så der kan føres kontrol med, om der sker rettidig afhjælpning. Den fagansvarlige eller anden person, som er udpeget til opgaven, bør løbende evaluere, om tilbageværende høj risiko bliver afhjulpet.

BILAG 1 – EKSEMPEL PÅ SKEMA FOR RISIKOVURDERING

Risikovurdering af [indsæt genstand for risikovurdering]											
Trussel	Beskrivelse af hændelse	Sårbarheder	**Sandsynlighed**		**Konsekvenser**						**Risiko**
					Fortrolighed		Integritet		Tilgængelighed		
			Begrundelse	Score	Begrundelse	Score	Begrundelse	Score	Begrundelse	Score	
1. Tab af enheder, lagermedier og dokumenter som indeholder personoplysninger	1.1. Tab af pc'er under transport fra eller til arbejde	• PC'er opbevares uden opsyn under transport (cykel, bil, tog eller bus) • PC'er er ikke krypteret • Der opbevares følsomme oplysninger på pc'er	Historik for tab af pc'er under transport	3	Mange typer af følsomme personoplysninger om den registrerede på pc (race, religiøs overbevisning og helbred) Tavshedsbelagte oplysninger (økonomi og sociale forhold)	3		2		2	**9**
	1.2. Tab af USB-stik mellem dataindsamling	• Svag kryptering • Ingen politik om brug af USB-stik og databeskyttelse	Historik for tab af USB-stik mellem dataindsamling	4	Mange typer af følsomme personoplysninger på USB-stik om mange registrerede	3		3		3	**12**

		• Der anvendes et stort antal USB-stik i brug ved data-indsamling • Ingen back-up fordi oplysninger endnu ikke er gemt i fagsystem							
2. Tyveri af enheder, lagermedier og dokumenter som indeholder personoplysninger	2.1. Enhed, lagermedie eller dokument stjæles i forbindelse med indbrud.	• Svag kryptering af enhed • Personfølsomme oplysninger opbevares på pc • Det sker at pc'er, usb-stik mv. opbevares i bagagerum i bil							
3. Uautoriseret adgang til systemer og personoplysninger	3.1. Der opnås uautoriseret adgang til system og data ændres	• Manglende adgangsstyring • Manglende kontrol med brugere og tildelte adgangsrettigheder • Ingen logning i it-systemer							
	3.2. Der opnås uautoriseret adgang til system og data tilintetgøres	• Manglende adgangsstyring • Manglende kontrol med brugere og tildelte adgangsrettigheder							
4. Videregivelse af personoplysninger til uvedkommende	4.1. Transmission af personoplysninger uden tunnelkryptering	• Ingen uddannelse af medarbejdere • Manglende teknisk understøttelse til							

		tunnelkrypte-ring									
5. Malware	5.1. Virus i syste-mer, enheder og lagerme-dier via mal-ware og kon-trol over data mistes	• Ingen firewall • Ikke opdateret virusbeskyt-telse • Ingen aware-ness omkring malware									

BILAG 2 – TYPER AF RISIKOVURDERINGER – ET OVERBLIK

Der findes flere forskellige typer af risikovurderinger og konsekvensanalyser. I skemaet nedenfor gives et overblik.

Type	Beskrivelse	Metode & værktøj
Risikovurdering		
Artikel 32	Forordningens artikel 32 indebærer, at der for hver behandlingsaktivitet skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau. Foranstaltningerne gennemføres på baggrund af en risikovurdering, som har fokus på konsekvenserne for de *registrerede* ved brud på fortrolighed, integritet og tilgængelighed.	F-Secure har i forbindelse med risikovurdering af it-systemet CURA udarbejdet en metode og et værktøj, som kan anvendes til risikovurdering.
Forretningsorienteret risikovurdering fra sikkerhedsstandarder f.eks. ISO 27001	Implementering og vedligeholdelse af ledelsessystem for informationssikkerhed (ISMS) anvender en forretningsorienteret risikoanalyse, hvor fokus er på konsekvenserne for *kommunen* ved brud på fortrolighed, integritet og tilgængelighed.	Typisk vil man bruge risikostyringsmetoden efter sikkerhedsstandarden ISO 27005 eller ISO 31000. Kombit har udarbejdet en metode og et værktøj til forretningsorienteret risikoanalyse og risikovurdering efter artikel 32 (hybrid risikovurdering)[4].
Konsekvensanalyse		
"DPIA Light"	En forenklet konsekvensanalyse udføres igennem et interview af den fagansvarlige og tillader at identificere de overordnede konsekvenser for de registrerede ved brud på fortrolighed, integritet og tilgængelighed.	F-Secures metode for kortlægning af behandlingsaktiviteter.
Artikel 35, Data Protection Impact Assessment (DPIA)	Formålet med DPIA'en, jf. artikel 35 i forordningen, er at kulegrave behandlingen og kortlægge alle risici for de registrerede, men så vidt muligt også at afhjælpe disse. Der skal udføres en DPIA før behandling af personoplysninger, hvis behandlingen sandsynligvis indebærer en høj risiko for de registreredes rettigheder og frihedsrettigheder.	F-Secure har i forbindelse med risikovurdering af it-systemet CURA udarbejdet en DPIA metode, som kan anvendes.

[4] Kombits metode og værktøj kan findes her: https://www.kombit.dk/indhold/gdpr-vejledninger-og-v%C3%A6rkt%C3%B8jer-%E2%80%93-eksempler-fra-kombit