Persónuvernd

Fræðsla fyrir starfsfólk Samgöngustofu

10. september 2025

Rakel Jensdóttir persónuverndarfulltrúi

Umfjöllun í dag

- Lög um persónuvernd og vinnslu persónuupplýsinga
- Hvað er "vinnsla persónuupplýsinga"?
- Hvenær er heimilt að vinna með persónupplýsingar?
- Hinar sex „gullnu reglur“ um vinnslu persónuupplýsinga
- Réttindi hinna skráðu
- Persónuvernd og gervigreind
- Nokkur praktísk atriði þegar unnið er með persónuupplýsingar

Persónuvernd

- **Lög nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga**
- GDPR reglugerðin
- Eldri lög nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga
- Í reynd ekki mikil breyting á því hvenær heimilt er að vinna með persónupplýsingar og hvernig á að fara með þær
- **Mikil breyting á utanaumhaldi í kringum vinnslu persónuupplýsinga**
  - Persónuverndarfulltrúar
  - Skylda til að tilkynna öryggisbrest
  - Skylda til að halda vinnsluskrá um alla vinnslu persónuupplýsinga
  - Skylda til að framkvæma MÁP

Vinnsla persónuupplýsinga

- **Vinnsla persónuupplýsinga**
- **Persónuupplýsingar:**
  - Allar upplýsingar sem hægt er að rekja til tiltekins einstaklings **beint eða óbeint**
  - Nafn, kennitala, fingrafar, mynd, DNA, dulkóðaðar upplýsingar, IP tala, bílnúmer o.fl.
- **Vinnsla:**
  - T.d. söfnun, skráning, skoðun, miðlun, breyting, eyðing, varðveisla, upptaka (hljóð eða mynd)
  - Munnleg miðlun skráðra upplýsinga

Almennar eða viðkvæmar persónuupplýsingar?

- **Almennar eða viðkvæmar persónupplýsingar?**
- Ríkari kröfur þegar unnið er með viðkvæmar persónuupplýsingar
  - Heilsufar, kynþáttur, þjóðerni, uppruni, trú, lífsskoðanir, stjórnmálaskoðanir, stéttarfélagsaðild, kynhneigð, erfðafræðilegar upplýsingar
  - Upplýsingar um refsiverða háttsemi
- **Upplýsingar viðkvæms eðlis?**
  - T.d. upplýsingar um fjárhagsmálefni og félagsleg vandamál
    - Upplýsingar sem fólk upplifir oft sem viðkvæmar
    - Aðgæsluskylda

Hvenær er heimilt að vinna með persónuupplýsingar?

- **Meginreglan er sú að það er óheimilt að vinna með persónuupplýsingar!**
- Nema ef til staðar er sérstök heimild í persónuverndarlögunum
- Misjafnar kröfur eftir því hvort verið er að vinna með almennar persónuupplýsingar eða viðkvæmar persónuupplýsingar
- Heimildir til vinnslu persónuupplýsinga:
  - **Almennar** persónuupplýsingar sbr. 9. gr. pvl.
  - **Viðkvæmar** persónuupplýsingar sbr. 9. gr. og 11. gr. pvl.
  - Upplýsingar um **refsiverða háttsemi** sbr. 12. gr. pvl.
- Mikilvægt að taka afstöðu til heimildar til vinnslu áður en vinnsla hefst

Heimild til að vinna með almennar persónuupplýsinar

1. **Samþykki**
2. Til að **efna samning** sem hinn skráði er aðili að
3. **Lagaskylda** sem hvílir á ábyrgðaraðila
4. Til að vernda **brýna hagsmuni** hins skráða eða annars einstaklings
5. Verk sem unnið er í þágu **almannahagsmuna** eða við **beitingu opinbers valds**
6. **Lögmætir hagsmunir** sem ábyrgðaraðili eða einhver annar gætir nema hagsmunir hins skráða vegi þyngra

Heimild til að vinna með viðkvæmar persónuupplýsingar

1. Afdráttarlaust samþykki

2. Til þess að ábyrgðaraðili/hinn skráði geti staðið við skuldbindingar sínar og nýtt sér tiltekin réttindi samkvæmt vinnulöggjöf eða löggjöf um almannatryggingar eða félagslega vernd.

3. Verulegir hagsmunir einstaklings eða annars einstaklings sem er ófær um að gefa samþykki.

4. Vinnsla hjá góðgerðastofnunum og sambærilegum aðilum.

5. Ef einstaklingur hefur sjálfur augljóslega gert upplýsingar opinberar.

6. Til að stofna, hafa uppi eða verja réttarkröfu eða þegar dómstólar fara með dómsvald sitt

7. Verulegir almannahagsmunir, á grundvelli laga

8. Til að fyrirbyggja sjúkdóma eða vegna atvinnusjúkdómalækninga

9. Almannahagsmunir á sviði lýðheilsu

10. Skjalavistun í þágu almannahagsmuna, rannsóknir á sviði vísinda eða sagnfræði eða í tölfræðilegum tilgangi

Heimild til þess að vinna með upplýsingar um refsiverða háttsemi

- Stjórnvöld mega ekki vinna með upplýsingar um refsiverða háttsemi nema það sé nauðsynlegt í þágu lögbundinna verkefna þeirra
- Einnig takmarkanir á miðlun til þriðja aðila, einkum:
  - Afdráttarlaust samþykki
  - Nauðsynlegt vegna lögmætra hagsmuna hins opinbera sem vega þyngra en hagsmunir hins skráða
  - Miðlun nauðsynleg svo hægt sé að taka stjórnvaldsákvörðun

„Gullnu reglurnar sex“

- Sex meginreglur um vinnslu persónuupplýsinga (8. gr. laga nr. 90/2018)

1. Sanngirnisreglan (lögmætisreglan)
2. Tilgangsreglan
3. Meðalhófsreglan
4. Áreiðanleikareglan
5. Varðveislureglan
6. Öryggisreglan

Sanngirnisreglan

- **Sanngirnisreglan:** að persónuupplýsingar séu unnar með lögmætum, sanngjörnum og gagnsæjum hætti
- Lýtur einkum að réttindum hins skráða, s.s. upplýsingarétti og aðgangsrétti
- Lögmæti vinnslunnar – Viðeigandi heimild til staðar fyrir vinnslunni

Tilgangsreglan

- **Tilgangsreglan:** að persónuupplýsingar séu unnar í skýrum, lögmætum og málefnalegum tilgangi og ekki unnar í öðrum og ósamrýmanlegum tilgangi
- Hvenær skal vinna með persónuupplýsingar?
- Það þarf að ákvarða tilgang með vinnslu fyrirfram
- Vinnsluskrá
- Mat á áhrifum á persónuvernd (MÁP)
- Má breyta?

Meðalhófsreglan

- **Meðalhófsreglan:** að persónuupplýsingar séu nægilegar, viðeigandi og ekki umfram það sem nauðsynlegt er miðað við tilganginn með vinnslu þeirra
- Ekki skrá meira en þörf er á
- Viðeigandi upplýsingar með hliðsjón af tilgangi vinnslu
- Nægilegar til þess að tilgangi sé náð
- Tengist tilgangsreglunni

Áreiðanleikareglan

- **Áreiðanleikareglan:** að persónuupplýsingar séu áreiðanlegar og uppfærðar eftir þörfum
- Persónuupplýsingum sem eru óáreiðnalegar eða ófullkomnar skal eyða eða þær leiðréttar án tafar
- Sérstök sjónarmið um ríkið

Varðveislureglan

- **Varðveislureglan:** að persónuupplýsingar séu varðveittar í því formi að ekki sé unnt að bera kennsl á einstaklinga lengur en þörf krefur miðað við tilganginn með vinnslu þeirra
- Undantekning – skjalavistun í þágu almannahagsmuna
- Skilaskylda til Þjóðskjalasafns

Öryggisreglan

- **Öryggisreglan:** að persónuupplýsingar séu unnar með þeim hætti að viðeigandi öryggi þeirra sé tryggt
- Ekki útfært í lögunum hvað sé „viðeigandi öryggi“
- Þeir sem vinna með persónuupplýsingar bera þannig ábyrgð á því að öryggi persónuupplýsinga sé tryggt.
- Helstu skyldur eru eftirfarandi:
  - Ekki sé hætta á að óviðkomandi aðilar komist í þær
  - Að þær skaðist ekki eða glatist
  - Að þeir sem hafa gilda ástæðu til, komist í upplýsingarnar
  - Öryggisráðstafanir skuli taka mið af umfangi og viðkvæmni gagnanna

Ábyrgðarskylda

- Ábyrgðaraðili er ábyrgur fyrir því að farið sé að reglum persónuverndarlaganna og þarf að geta sýnt fram á það á hverjum tíma
- Ábyrgðaraðili þarf að gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að sýna fram á reglufylgni (skjölun)
  - Skjalfestar verklagsreglur innanhúss um meðferð persónuupplýsinga
  - Halda skrá yfir öryggisfrávik
  - Vinnsluskrá
  - Áhættumat – öryggisráðstafanir
  - Mat á áhrifum á persónuvernd (MÁP)
  - Persónuverndarfulltrúi

Réttindi hinna skráðu

1. Réttur til að fá fræðslu um vinnslu persónuupplýsinga
2. Réttur til aðgangs að eigin upplýsingum
3. Réttur til leiðréttinga á óáreiðanlegum/röngum upplýsingum
4. Réttur til eyðingar og að vinnsla verði takmörkuð
5. Réttur til að flytja eigin gögn
6. Andmælaréttur
7. Réttindi tengd einstaklingsmiðuðum ákvörðunum sem byggja á sjálfvirkri gagnavinnslu (gervigreind)

Fræðsluskyldan

- Ábyrgðaraðili á að veita hinum skráða fræðslu um þá vinnslu persónuupplýsinga sem fer fram hjá honum um hinn skráða
- Ábyrgðaraðili ákveður hvernig hann gerir þetta
- Ábyrgðaraðili ber sönnunarbyrði um að fræðsluskyldu hafi verið sinnt
- Fræðsluskylda sérstaklega mikilvæg þegar unnið er með viðkvæmar persónuupplýsingar
- **Undantekning:** Á ekki við þegar stjórnvald miðlar upplýsingum til annars stjórnvalds á grundvelli lagaheimildar

Upplýsingaréttur hins skráða

- Hinn skráði á rétt á því að fá upplýsingar um það hvaða persónuupplýsingar ábyrgðaraðili vinnur um hann
- Beiðni skal að jafnaði afgreiða innan mánaðar
- Sérstök sjónarmið þegar stjórnvald vinnur með upplýsingar
  - Á ekki við vinnuskjöl sem notuð eru við undirbúning ákvarðana
  - Persónuverndarlögin takmarka ekki þann rétt sem einstaklingar eiga nú þegar samkvæmt öðrum lögum
  - Réttur aðila máls til aðgangs að gögnum samvkæmt stjórnsýslulögum
  - Upplýsingaréttur almennings samkvæmt upplýsingalögum

Réttur til leiðréttingar

- Einstaklingur á að jafnaði rétt á að ábyrgðaraðili leiðrétti óáreiðanlegar upplýsingar um hann
- Takmarkað vægi þegar stjórnvöld eiga vinna með persónuupplýsingar – þess vegna mikilvægt að skrá réttar upplýsingar
- Lagaskylda til þess að varðveita upplýsingar – lög um opinber skjalasöfn
  - Endanlega ákvörðun eða gögn
  - Röng skráning í kerfi opinberra aðila

Rétturinn til eyðingar

- Einstaklingar geta krafist þess að upplýsingum um þá verði eytt:
  - Draga til baka samþykki fyrir vinnslu
  - Vinnsla persónuupplýsinga ekki lengur nauðsynleg
  - Vinnsla persónuupplýsinga var ólögmæt
  - Stjórnvöld þurfa að fá samþykki þjóðskjalavarðar

Persónuvernd og gervigreind

- Ekki fjallað um gervigreind í persónuverndarlöggjöfinni
- ATH þó 22. gr. laga nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga:
- *“Skráður einstaklingur skal eiga rétt á því að ekki sé tekin ákvörðun eingöngu á grundvelli sjálfvirkrar gagnavinnslu, þ.m.t. gerðar persónusniðs, sem hefur réttaráhrif að því er hann sjálfan varðar eða snertir hann á sambærilegan hátt að verulegu leyti…”*
- Einstaklingur á almennt rétt á mannlegri íhlutun þegar teknar eru ákvarðanir sem varða hann
  - T.d. lánshæfismat, skattákvarðanir, synjun um bætur

Persónuvernd og gervigreind

- Persónuverndarlöggjöfin gildir um alla vinnslu persónuupplýsinga
- Mörg álitaefni sem koma upp varðandi persónuvernd og gervigreind
  - Hver er ábyrgðaraðili og vinnsluaðili – hefur verið gerður vinnslusamningur?
  - Heimild til vinnslu?
  - Hvernig á að uppfylla fræðsluskylduna?
  - Vitum við hvað verður um upplýsingar? Gagnsæi við vinnslu persónuupplýsinga
  - Réttur til aðgangs?
  - Einstaklingur á rétt á að draga samþykki fyrir vinnslu persónuupplýsinga til baka
  - Rétturinn til að leiðrétta rangar/óáreiðanlegar persónupplýsingar
  - Ábyrgðaraðili þarf alltaf að geta sýnt fram á að vinnsla persónuupplýsinga sé í samræmi við lög

Persónuvernd og gervigreind

- Margir farnir að nota gervigreind í störfum sínum
- Ef stjórnvöld ætla að byrja að nota gervigreind í starfsemi sinni er mikilvægt að framkvæma mat á áhrifum á persónuvernd áður en slík vinnsla hefst
- Margar stofnanir nú þegar farnar að móta sér stefnu um notkun gervigreindar
- Sýna varfærni og ekki hlaða inn persónugreinanlegum gögnum í opnar lausnir

Persónuvernd og gervigreind

Nokkur praktísk atriði sem gott er að hafa í huga þegar unnið er með persónuupplýsingar

Hvar erum við að vinna með persónuupplýsingar?

- Öryggi að jafnaði mest þegar unnið er með upplýsingar inni í kerfum stofnunar
- Meiri áhætta:
  - Gögn afrituð úr kerfum, t.d. excel skjöl
  - Pappír
  - USB lyklar
  - Heimavinna/ferðalög

Er öruggt að senda persónuupplýsingar með tölvupósti?

- Tölvupóstur er almennt ekki talinn öruggur farvegur fyrir miðlun persónuupplýsinga án frekari ráðstafana
  - Á sérstaklega við um viðkvæmar persónuupplýsingar
  - Senda gögn í gegnum SignetTransfer
  - Hægt að lágmarka hættuna t.d. með því að senda læsta skrá og lykilorð í SMS
  - Ábyrgðarpóstur
- Hætta á að senda á rangan aðila
- Sérstök varúð ef tölvupóstur er sendur á marga einstaklinga (cc og bcc)

Hvernig á að bregðast við öryggisbresti?

- **Öryggisbrestur** er brestur á öryggi sem leiðir til óviljandi eða ólögmætrar eyðingar persónuupplýsinga, sem eru sendar, varðveittar eða unnar á annan hátt, eða að þær glatist, breytist, verði birtar eða aðgangur veittur að þeim í leyfisleysi.
- Ábyrgðaraðili á að halda skrá yfir öryggisbresti þar sem fram kemur hvernig brugðist var við atviki
- Þarf að tilkynna til Persónuverndar innan 72 klst nema ólíklegt sé að bresturinn leiði til áhættu fyrir réttindi og frelsi einstaklinga
- Þarf að tilkynna einstaklingi ef líklegt er að brestur leiði af sér mikla áhættu fyrir réttindi og frelsi hans

Hvernig á að bregðast við öryggisbresti/fráviki?

- **Öryggisbrestur/öryggisfrávik**
- Utanaðkomandi ógn og mannleg mistök
- **Dæmi:**
  - Tölvuárás
  - Bilun í kerfi
  - Upplýsingum óvart eytt
  - Upplýsingar fara á flakk (pappír, usb lyklar….)
  - Upplýsingar birtar fyrir röngum viðtakanda
  - Upplýsingar birtar opinberlega fyrir mistök
- Bregðast strax við og reyna að lágmarka skaðann og tilkynna til persónuverndarfulltrúa

Spyrjum ef við erum í vafa

- Ef spurningar vakna eða ef þið þurfið ráðleggingar:
- personuvernd@samgongustofa.is

Takk fyrir!