

Ný persónuverndarlög
áskoranir tengdar skjala- og upplýsingastjórn

Fræðslufundur Félags um skjalastjórn 22.02.2018

Ásgerður Kjartansdóttir
Skjalastjóri Landsnets

Dagskrá

- Nokkur grunnatriði nýrra persónuverndarlaga
- Helstu áhrif á skjala- og upplýsingastjórn
- Vinnsluskrá
- Vegferð Landsnets við innleiðingu

Hvað eru persónuupplýsingar?

- Persónugreindar upplýsingar – upplýsingar sem hægt er að rekja beint með nafni einstaklings eða öðru auðkenni sem augljóslega tilheyrir honum
nafn, kennitala
- Persónugreinanlegar upplýsingar – þá er hægt að rekja upplýsingarnar til einstaklings þótt þær séu ekki sérstaklega merktar honum
dæmi: bílnúmer, símanúmer, IP-tala
- Viðkvæmar persónuupplýsingar – um uppruna, litarhátt, kynþátt, stjórnmalaskoðanir, trúar- eða aðrar lífsskoðanir, heilsuhagi, kynhegðan, séttarfélagsaðild og hvort viðkomandi hafi verið grunaður, ákærður eða dæmdur fyrir refsiverðan verknað

Ný persónuverndarlög

Grunnatriði

- Tilgangur vinnslu persónuupplýsinga
- Lögmæti vinnslu – lagaskylda / samningur / samþykki
- Réttur einstaklingsins
 - til að fá aðgang að upplýsingum
 - til að leiðrétta upplýsingar
 - takmarka /andmæla vinnslu
 - flytja eigin gögn
 - eyða gögnum
- Persónuverndarstefna / -reglur
- Öryggi við vinnslu persónuupplýsinga
- Vinnsluskrá

Áskoranir

- Skýr og afmarkaður tilgangur. Gæta meðalhófs og biðja eingöngu um það sem er nauðsynlegt
- Lögmæti vinnslu skýrt – ef vinnsla byggir á samþykki þarf það að **vera rekjanlegt – halda vel utan um allt sem einstaklingar samþykkja**
- Réttur einstaklingsins - ríkar skyldur til skráningar og utanumhalds. Kallar á skýrt verklag við móttöku og umsýslu beiðna
- Rík fræðsluskylda um hvaða upplýsingum er safnað og í hvaða tilgangi
- Áhættumeta þarf UT-kerfi og vinnslu persónuupplýsinga – innra eftirlit. Viðbrögð við öryggisbroti – tilkynningaskylda
- Vinnsluskrá - útvíkka skjalastjórnaráætlun þannig að hún nái til persónuupplýsinga?

Vinnsluskrá

Skrá yfir alla vinnslustarfsemi sem á sér stað og tengist persónuupplýsingum

- Tilgangur vinnslu
- Lýsing á flokkum skráðra einstaklinga
- Lýsing á flokkum persónuupplýsinga
- Tímamörk varðandi eyðingu – ef slíkt er leyfilegt
- Lýsing á öryggisráðstöfunum

Kortlagning UT kerfa – data map

LANDSNET

Þjónusta	Hugbúnaður/Vélbúnaður/Fjarskiptastaðir	PU	Svið vörustjóra	Vörustjóri	Tæknitengiliður	Þjónustuaðili
Farsímar	Mínar Síður Vodafone	x	Kerfisstjórnunarsvið	Bergþór Sveinsson	Bergþór Sveinsson	Vodafone
Ferðabæiðakerfi	Habilis	x	Fjármálasvið	Guðlaug Sigurðardóttir	Helgi Pétur Gunnarsson	Habilis
Ferilvöktun	Sitewatch	x	Framkvæmda- og rekstrarsvið	Ragnar Guðmannsson	Bergþór Sveinsson	Samsýn
Fjárhagsbókhald	DynAX	x	Fjármálasvið	Kristín Halldórsdóttir	??	Annata
Fjárstýringarkerfi	IFS (Treasury)	nafn, netfang	Fjármálasvið	Inga Guðmundsdóttir	Bergþór Sveinsson	IFS
Fundarherbergisskjár í móttöku	Agentus	x	Stjórnunarsvið	Kristbjörg Kristjánsdóttir	Bergþór Sveinsson	Rögg
Innkaup	DynAX	x	Fjármálasvið	Kristín Halldórsdóttir	??	Annata
Innri vefur	Lisa (innranet)	x	Stjórnunarsvið	Steinunn Þorsteinsdóttir	Bergþór Sveinsson	Advania
Innri vefur - Facebook Workplace	Facebook Workplace	x	Stjórnunarsvið	Steinunn Þorsteinsdóttir	????	
Innskil áætlana	Amper	x	Kerfisstjórnunarsvið	Teitur Birgisson	Helgi Pétur Gunnarsson	Kerfisstjórnunarsvið
Innskráning gesta	Visita	x	Stjórnunarsvið	Kristbjörg Kristjánsdóttir	Bergþór Sveinsson	Advania
Launakerfi	H3	x	Fjármálasvið	Valka Jónsdóttir	Guðmundur Guðmundsson	Tölvumiðlun
Ljósmyndasafn	FotoWeb	nafn starfsmanns	Stjórnunarsvið	Ásgerður Kjartansdóttir	Guðmundur Guðmundsson	Þekking
Mannauðskerfi	H3	x	Fjármálasvið	Valka Jónsdóttir	Guðmundur Guðmundsson	Tölvumiðlun

Vinnsluskrá Landsnets

Svið/ eining	Verkefni	Tengiliður	Kerfi	Sameiginlegur ábyrgðaraðili	Hinir skráðu	Persónuupplýsingar	Sérstakir flokkar persónuupplýsinga/ viðkvæmar persónuupplýsingar	Aðal tilgangur vinnslu	Lögmæti vinnslu og rökstuðningur	Hafa hinir skráðu fengið fræðslu um vinnsluna?	Viðtakendur	Vinnsluaðili	Miðlun til þriðju landa? Grundvöllur?	Öryggis-ráðstafanir	Vardveislu-tími
Mannauður	Ráðningarferli - umsóknir	Mannauðsstjóri	H3, Askur, [heimasiða e ef við á]	NA	Umsækjendur	<p>Upplýsingar sem Landsnet óskar eftir: Tengiliðaupplýsingar, s.s. kennitala, nafn, netfang, heimilisfang og símanúmer. Upplýsingar um kyn, reykingar, fyrri störf og ástæðu umsóknar. Upplýsingar um menntun og námskeið, tungumálakunnátta, kunnátta á Word og Excel, önnur kunnátta. Starfsferill, umsagnaraðilar.</p> <p>Upplýsingar sem umsækjendur velja að afhenda: Áhugamál, ferilskrá, kynningarbréf, upplýsingar um fjölskylduhagi o.s.frv.</p>	NA	<p>Kanna feril umsækjenda um störf. Velja hæfasta umsækjandan.</p> <p>Nauðsynleg til að gera ráðstafanir að beiðni hins skráða áður en samningur er gerður, sbr. 2. tl. 1. mgr. 8. gr. pvl., sbr. b-lið 1. mgr. 6. gr. GDPR.</p> <p>Vinnsla byggist að hluta einnig á lagaskyldu, sbr. 3. tl. 1. mgr. 8. gr. pvl. og c-lið 1. mgr. 6. gr. GDPR.</p>	[Áður en umsókn er send inn er persónuverndarstefna félagsins varðandi umsækjendur birt umsækjanda á heimasíðu Landsnets.]	NA	[Ef við á tilgreina ráðningaskrifstofu].	NA	Aðgangsstýringar. [Landsnet fyllir inni ef fleiri ráðstafanir eiga við.]	Ótímabundið á grundvelli laga um opinber skjalasöfn.	
Mannauður	Ráðningarferli - sakavottorð	Mannauðsstjóri	[Landsnet fyllir út]	NA	Umsækjendur sem komast áfram í valferli. [Landsnet ath. tilgreina þau störf sem um ræðir?]	Innihald sakavottorðs	Upplýsingar um innihald sakavottorðs.	<p>Kanna feril umsækjenda um störf. Velja hæfasta umsækjandan.</p> <p>Vinnslan byggir á samþykki hins skráða sbr. 1. tl. 1. mgr. 8. gr. og 1. tl. 1. mgr. 9. gr. pvl., sbr. og a-liður 1. mgr. 6. gr. og a-liður 2. mgr. 9. gr. GDPR.</p> <p>[Hvernig er samþykkið fengið?]</p>	[Tillaga: Umsækjendur fá fræðslu á samþykkiseyðublaði. Einnig koma fram almennar upplýsingar um vinnslu persónuupplýsinga í persónuverndarstefnu félagsins um umsækjendur.]	NA	NA	NA	[Landsnet fyllir út]	Ótímabundið á grundvelli laga um opinber skjalasöfn.	

Vegferð Landsnets við innleiðingu

LANDSNET

Ágúst 2017

Vinnuhópur skipaður
Undirbúningur úttektar

Sept.-okt.

Úttekt á vinnslu persónuupplýsinga
Forgangsröðun úrbóta

Nóv.-des.

Kortlagning á UT kerfum sem hýsa persónuupplýsingar
Persónuverndarreglur (3)

Janúar 2018

Fræðsla fyrir stjórnendur og þá sem sýsla með persónuupplýsingar
Kortlagning á nauðsynlegum breytingum

Febrúar - mars



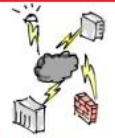










Fræðsla fyrir stjórnendur og þá sem sýsla með persónuupplýsingar
Breytingar á verklagi
Vinnsluskrá og vinnslusamningar

Apríl - maí



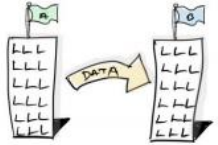


Innleiðing
Fræðsla

High level view of the GDPR





What organizations have to do

 <p>Keep records of all processing of personal information</p>	 <p>Institute safeguards for cross-border data transfers</p>	 <p>Maintain appropriate data security</p>	 <p>Collect personal data lawfully and fairly, and where relevant, get appropriate consent and provide notification of personal data processing activities</p>	 <p>Get a parent's consent to collect data for children under 16</p>	 <p>Consult with regulators before certain processing activities</p>	 <p>Provide appropriate data protection training to personnel having permanent or regular access to personal data</p>
 <p>Conduct Data Protection Impact Assessments on new processing activities</p>	 <p>Implement Data Protection-by-Design (Privacy "baked-in")</p>	 <p>Take responsibility for the security and processing activities of third-party vendors</p>	 <p>Appoint a Data Protection Officer (if you regularly process lots of data or particularly sensitive data)</p>	 <p>Be able to demonstrate compliance on demand</p>	 <p>Notify data protection agencies and affected individuals of data breaches in certain circumstances</p>	

What individuals can do

 <p>Withdraw consent for processing</p>	 <p>Request a copy of all of their data & request corrections if wrong</p>	 <p>Request the ability to move their data to a different organization</p>
 <p>Request that their information is deleted when there's no purpose to retain it</p>	 <p>Object to automated decision-making processes, including profiling</p>	

What regulators can do

 <p>Ask for records of processing activities and proof of steps taken to comply with the GDPR</p>	 <p>Suspend cross-border data flows</p>
 <p>Impose temporary data processing bans, require data breach notification, or order erasure of personal data</p>	 <p>Enforce penalties of up to €20 million or 4% of annual revenues for non-compliance</p>

Inspired by IAPP's GDPR Awareness Guide. Please credit Tim Clements & IAPP if you use this

<https://irp-cdn.multiscreensite.com/3fdd5caa/files/uploaded/GDPR%20high%20level%20view.pdf>