Persónuvernd hjá OR

Innleiðing á PVRG 2018

Íris Lind Sæmundsdóttir, lögfræðingur

Kynning á fræðslufundi faghóps Stjórnvísi um persónuvernd

19. september 2018

Ný persónuverndarlöggjöf 2018

- Persónuvernd er hluti EES samningsins

- PVRG / GDPR - Reglugerð ESB 2016/679
  - Almenna persónuverndarreglugerðin
  - Samþykkt 27. apríl 2016
  - Kom til framkvæmda í ESB 25. maí 2018
  - Tekin upp í EES samninginn 6. júlí 2018

- Lög um persónuvernd og vinnslu persónuupplýsinga
  - Lög nr. 90/2018
  - Gildistaka 15. júlí 2018
  - Með þeim öðlaðist PVRG lagagildi á Íslandi

Orkuveita Reykjavíkur

Aukinn réttur einstaklinga

- Eitt meginmarkmiða GDPR er að veita einstaklingum betri vernd og færa þeim aukinn ákvörðunarrétt yfir sínum persónuupplýsingum.
  - Fela þeim stjórn yfir því hver vinnur upplýsingar um þá, hvenær og í hvaða tilgangi.
- Auknar og strangari skyldur lagðar á lögaðila.
  - Skulu m.a. upplýsa einstaklinginn um vinnslu persónuupplýsinga sem á sér stað.
  - Og gera þeim grein fyrir því með hvaða hætti staðið er að því að tryggja öryggi þeirra.

Orkuveita Reykjavíkur

Samstæða OR – Móðurfélag og 3 dótturfélög – 511 starfsmenn

VEITUR

Hitaveita, vatnsveita, rafveita og fráveita

GAGNAVEITA REYKJAVÍKUR

Háhraða gagnaflutningskerfi

ON ORKA NÁTTÚRUNNAR

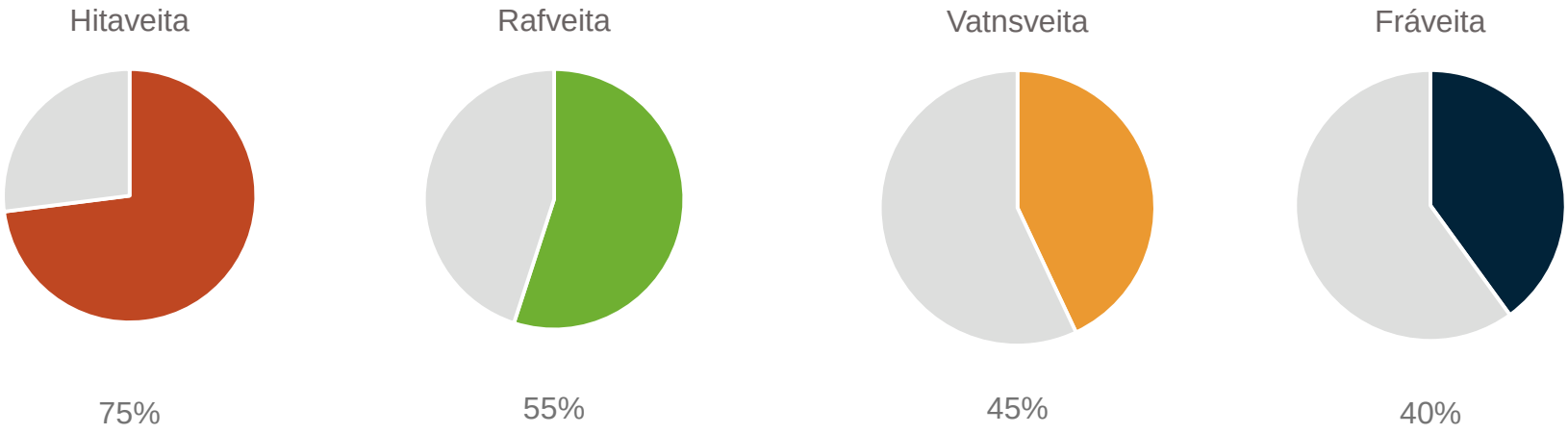
Framleiðsla og sala raforku

OR Orkuveita Reykjavíkur

Viðskiptavinir samstæðu OR fjölmargir

75.000 virkir viðskiptavinir Veitna

- Hlutfall Íslendinga sem Veitur þjóna



Orkuveita Reykjavíkur

Innleiðing hjá OR

1. Undirbúningur hefst óformlega 2016
2. Vinnuhópur skipaður innan samstæðu 2017
   - Fulltrúar frá dótturfélögum og starfseiningum ásamt lögfræðingi
3. Persónuupplýsingaeignir OR rýndar og skráðar haustið 2017
   - Nokkur skörun við ISO 27001 (upplýsingaöryggisstjórnunarstaðall)
     - Upplýsingaeignir ISO 27001 því lagðar til grundvallar
   - Mat á persónuupplýsingaeignum í kerfinu
     - Viðkvæmar persónuupplýsingar?
     - Hvar eru heimildir fyrir skráningunni?
     - Hver er tímalengd vistunar gagna?
     - Hvernig er aðgangsstýringu háttað?
     - Eru unnin einhver gögn upp úr safninu?
     - Hver er tilgangur vistunar upplýsinganna?
     - Hvernig er upplýsingum eytt?
     - Hvar er eyðing upplýsinga skráð?
     - Hvaða ferlar tengjast upplýsingasafninu?
   - Viðskiptavinir OR – innri (starfsmenn) og ytri (viðskiptavinir, birgar, verktakar og starfsmenn þeirra)

Orkuveita Reykjavíkur

Innleiðing hjá OR (frh.)

4. Skimun hefst á ferlum um áramót 2017 til júní 2018
   - Úrbætur / nýmæli þar sem þurfti
   - Rekstrarhandbók uppfærð samhliða rýninni
5. Námskeið fyrir starfsmenn í apríl 2018
6. Persónuverndarstefna samþykkt í stjórnum í maí 2018
7. Heimasíða og innra vefsvæði uppfært í maí 2018
   - Persónuverndarstefna
   - Greinargerð um vinnslu
   - Aðgangsrétturinn og eyðublað
8. Persónuverndarfulltrúi skipaður í júní 2018
   - Hörður Helgi Helgason, lögmaður á Landslögum

Orkuveita Reykjavíkur

Að tryggja að vinnsla samræmist PVRG

Persónuverndarstefna og ráðstafanir á grv. hennar

- Ábyrgðaraðili skal gera viðeigandi tæknilegar og skipulagslegar ráðstafanir til að tryggja og sýna fram á að vinnsla samræmist GDPR.
  - M.a. innleiða viðeigandi persónuverndarstefnu
    - 24. gr. rgl.
- Til að geta sýnt fram á farið sé að GDPR ætti ábyrgðaraðili að setja sér stefnu og innleiða ráðstafanir sem fylgja einkum meginreglunum um innbyggða persónuvernd og sjálfgefna persónuvernd.
    - Aðfararorð rgl.

Orkuveita Reykjavíkur

Lagskipt nálgun innan OR samstæðu

Stefna og ráðstafanir – þrjú lög

1. Almenn persónuverndarstefna (stefnan)
   - Ein stefna gildir fyrir alla (viðskiptavini, starfsmenn, birgja, verktaka, osfrv.)
   - Samþykkt í stjórn OR 28. maí 2018 https://www.or.is/um-or/starfsemi/personuverndarstefna
   - Samþykkt í stjórn ON 17. maí 2018 https://www.on.is/personuverndarstefna
   - Samþykkt í stjórn GR 18. maí 2018 https://www.ljosleidarinn.is/personuverndarstefna
   - Samþykkt í stjórn Veitna 22. maí 2018 https://www.veitur.is/personuverndarstefna

Orkuveita Reykjavíkur

Lagskipt nálgun innan OR samstæðu

(frh.)

2. Greinargerð:
   - Almenn ákvæði um innleiðingu stefnu (stefnan)
   - Aðskilin greinargerð fyrir hvernig hóp (viðskiptavinir / Starfsmenn)
     - https://www.or.is/sites/or.is/files/greinargerd_um_vinnslu_or_a_personuupplysingum.pdf
   - Upplýsingagjöf um þau atriði sem ber að upplýsa um
     - Almennar upplýsingar um OR
     - Hvaða upplýsingar eru unnar (flokkar / tegundir)
     - Tilgangur vinnslu
     - Viðtakendur upplýsinga (innan / utan OR)
     - Miðlun upplýsinganna til annars ríkis ef við á
     - Vistunartími - viðmið
     - Réttur til aðgangs, leiðréttingar, eyðslu, takmörkunar á vinnslu, andmælaréttur
     - Réttur til að draga samþykki til baka (ef við á)
     - Réttur til að kvarta til Persónuverndar

Orkuveita Reykjavíkur

Lagskipt nálgun innan OR samstæðu

(frh.)

3. Rekstrarhandbók (ráðstafanirnar)
   - Sértæk skjöl um einstaka vinnslu þar sem við á
     - Rafræn vöktun t.d.
   - Leiðbeiningar og verkferlar
     - Öryggisbrot, aðgangsréttur, mat á áhrifum á persónuvernd,

Orkuveita Reykjavíkur

Persónuverndarstefna OR

- Samþykkt 28. maí 2018

Öll meðferð OR á persónuupplýsingum lýtur lögum um persónuvernd og vinnslu persónuupplýsinga og reglum sem settar eru samkvæmt þeim. OR gætir þess að öll vinnsla persónuupplýsinga innan fyrirtækisins sé í samræmi við framangreind lög og tryggir að vinnsluaðilar sem fá aðgang að persónuupplýsingum fylgi þeim einnig.

OR upplýsir einstaklinga um þá vinnslu persónuupplýsinga sem á sér stað á vegum fyrirtækisins og í hvaða tilgangi hún er unnin. OR tryggir að vinnsla fari ekki fram í öðrum tilgangi en upplýst hefur verið um nema með fullri vitneskju og eftir atvikum með samþykki hlutaðeigandi.

Einstaklingar geta óskað upplýsinga um vinnslu sem á sér stað hjá OR og varðar þá sjálfa. Þeir geta andmælt henni telji þeir að hún samræmist ekki gildandi lögum og reglum og eftir atvikum krafist þess að röngum, villandi eða ófullkomnum persónuupplýsingum um sig verði eytt.

Orkuveita Reykjavíkur

Greinargerð OR um vinnslu (viðskiptavinir)

Greinargerð um vinnslu OR á persónuupplýsingum

1. Almennt

Orkuveita Reykjavíkur og dótturfélög hennar starfa skv. lögum nr. 136/2013 um Orkuveitu Reykjavíkur. Fyrirtækin stunda vinnslu, framleiðslu og sölu raforku og heits og kalds vatns og gufu og rekstur grunnkerfa, svo sem dreifiveitu rafmagns, hitaveitu, vatnsveitu, fráveitu og gagnaveitu, auk annarrar starfsemi sem hefur sambærilega stöðu. Þessa vöru og þjónustu selur OR viðskiptavinum gegn greiðslu.

Á milli OR og viðskiptavina er samninggssamband um veitingu á vöru og eða þjónustu. Svo unnt sé að veita og afhenda hana þurfa fyrirtækin að afla, skrá, vista og vinna persónuupplýsingar um viðskiptavini svo OR geti uppfyllt skyldur sínar gagnvart viðkomandi viðskiptavini. Ekki er um vinnslu viðkvæmra persónuupplýsinga að ræða.

Gagnvart viðskiptavini ábyrgist OR að öll vinnsla persónuupplýsinga af hálfu fyrirtækisins samræmist persónuverndarstefnu OR, lögum um persónuvernd og vinnslu persónuupplýsinga og reglum sem settar eru samkvæmt þeim. Í skjali þessu sem sett er til fyllingar stefnunni er að finna upplýsingar og fræðslu um þau atriði sem OR ber að veita vegna öflunar og vinnslu persónuupplýsinga um viðskiptavini.

2. Tilgangur vinnslu persónuupplýsinga um viðskiptavini

OR safnar og vinnur tilgreindar persónuupplýsingar um viðskiptavini í þeim tilgangi að geta veitt honum þá vöru og þá þjónustu sem samið er um að OR veiti og innheimt fyrir þá þjónustu áskilið endurgjald. Einnig svo unnt sé að tryggja ætíð bæði bestu mögulegu gæði vöru og þjónustu.

Einnig kann að vera unnið með persónuupplýsingar í þeim tilgangi að greina markaðsleg tækifæri með það fyrir augum að bjóða viðbótar þjónustu eða nýja þjónustu.

Tilgangur með vinnslu persónuupplýsinga getur einnig verið annar en greint er frá hér að framan. Til dæmis heldur OR úti rafrænni vöktun þar sem tilgangurinn er sértækur hverju sinni en slík vinnsla fer einkum fram til að tryggja öryggi starfsmanna, gæði þjónustu OR og í öryggis- og eignavörsluskyni: Myndavélaeftirlit í og við mannvirki OR, símavöktun í þjónustuveri, ökuritar í bifreiðum OR og með talstöðvum á Tetra samskiptakerfinu. Um rafræna vöktun gilda reglur persónuverndar um rafræna vöktun og leiðbeiningarskjöl í rekstrarhandbók OR, en þar er fjallað m.a. um tilgang vöktunar hverju sinni, hverjir sæti henni, hvar og hvenær henni er beitt, hverjar skyldur OR eru í þeim efnum og hver réttindi starfsmanns eru.

OR ábyrgist að persónuupplýsingar um viðskiptavini verði ekki notaðar í öðrum tilgangi en þeim sem afmarkaður er hér að framan nema með fullri vitneskju og eða samþykki viðskiptavinar.

3. Á hvaða heimild byggir vinnsla persónuupplýsinga um viðskiptavini

Vinnsla persónuupplýsinga um viðskiptavini er einkum nauðsynleg vegna framkvæmdar á samningi milli OR og viðkomandi einstaklings um veitingu fyrirtækisins á vöru og eða þjónustu. Að auki kann einhver vinnsla að byggjast á lögum, t.a.m. lögum um opinber skjalasöfn nr. 77/2014, lögum um bókhald nr. 145/1994 og lögum um ársreikninga nr. 3/2006.

Orkuveita Reykjavík
Bæjarhálsi 1 - 110 Reykj
Sími - Tél. +354 516 6
www.o

Þar sem samþykki er grundvöllur vinnslu persónuupplýsinga um viðskiptavini, gilda um það sérstakir skilmálar sem viðskiptavinur hefur undirgengist þegar hann veitti samþykkið. Slíkum skilmálum verður ekki breytt nema að fengnu samþykki viðskiptavinar.

4. Tegund persónuupplýsinga sem unnið er með

OR safnar og vinnur einkum úr eftirfarandi upplýsingum um viðskiptavini:

a. Nafn
b. Kennitala
c. Heimilisfang
d. Símanúmer
e. Netfang
f. Bankareikninga
g. Greiðslukortaupplýsingar sem eru dulkóðaðar í sólarhring og svo eytt
h. Notkunarsaga – álestrar/reikningar
i. Bilanasaga -rekstrartruflanir
j. Vanskilaupplýsingar
k. Samskiptaupplýsingar
l. Umsóknir um þjónustu/vöru (t.d. heimlagnir, ljósleiðara, afsal á vatns- og fráveitulögnum o.s.frv.)
m. Hljóðritanir símtala í þjónustuver OR
n. Gæslumyndavélar á almennum svæðum í og við starfsstöðvar
o. Fjarskiptaupplýsingar vegna viðskiptavina GR

Þegar viðskiptavinur á í samskiptum við OR á samfélagsmiðlum, t.d. skilar þar álestri eða öðrum upplýsingum, gilda reglur viðkomandi miðils um vernd og vistun persónuupplýsinga. Þar sem við á færir OR viðkomandi samskipti / upplýsingar yfir í sín kerfi og fer þar um vernd og vistun þeirra skv. persónuverndarstefnu OR og reglum settum til innleiðingar á henni.

5. Viðtakendur persónuupplýsinga um viðskiptavini

Upplýsingar um viðskiptavini eru vistaðar hjá OR eða á vegum fyrirtækisins á Íslandi eða hjá samstarfsaðila innan EES-svæðisins þar sem reglur um meðferð persónuupplýsinga eru þær sömu og á Íslandi. Persónuupplýsingar verða ekki afhentar þriðja aðila nema á grundvelli lagaheimildar, stjórnvaldsfyrirmæla, dómsúrskurðar, vinnslusamnings eða samþykkis viðskiptavinar.

6. Varðveislutími - Hversu lengi persónuupplýsingar um viðskiptavini eru varðveittar

OR vistar persónuupplýsingar um viðskiptavini í þann tíma sem lög gera ráð fyrir og nauðsynlegt er m.v. tilgang vinnslunnar. Þar sem OR er í eigu opinberra aðila lýtur fyrirtækið lögum um opinber skjalasöfn og ber því varðveislu- og skilaskyldu samkvæmt þeim. Eru fyrirtækinu því ákveðnar hömlur settar hvað eyðingu gagna varðar. Þeim gögnum sem heimild stendur til að eytt verði skv. sérstöku leyfi Borgarskjalasafns verður eytt í samræmi við veitta heimild hverju sinni.

7. Réttur viðskiptavinar til andmæla, til aðgangs, leiðréttingar og eyðingar/takmörkunar vinnslu

Viðskiptavinur hefur rétt til að andmæla söfnun OR á persónuupplýsingum telji hann að hún samræmist ekki tilgangi hennar, meðalhófs sé ekki gætt eða ef hann telur að ná megi sama tilgangi með vægari hætti.

2

Viðskiptavinur getur óskað eftir því að fá upplýsingar um þá vinnslu sem á sér stað hjá OR um hann enda standi hagsmunir annarra ekki í vegi fyrir því. Beiðni þar um skal afgreidd eins fljótt og auðið er og ekki síðar en innan mánaðar frá móttöku beiðni viðskiptavinar þar um.

Viðskiptavinur kann að eiga rétt á að krefjast þess að röngum, villandi eða ófullkomnum persónuupplýsingum um sig verði leiðréttar og eða þeim eytt.

8. Réttur viðskiptavinar til að leggja fram kvörtun og athugasemdir

Vilji viðskiptavinur koma andmælum, kvörtun eða athugasemdum á framfæri vegna vinnslu persónuupplýsinga skal henni beint að fyrirtækinu. Sé ekki brugðist við af hálfu viðkomandi einingar getur viðskiptavinur leitað til persónuverndarfulltrúa samstæðu OR, personuverndarfulltrui@or.is (sjá nánar hér að neðan).

Viðskiptavini er einnig heimilt að bera vinnslu persónuupplýsinga undir Persónuvernd (www.personuvernd.is)

9. Nákvæmni og áreiðanleiki upplýsinga

OR ber ábyrgð á áreiðanleika upplýsinga og að upplýsingar um viðskiptavin séu ávallt uppfærðar í samræmi við tilkynningar hans um breytingar og að teknu tilliti til tilgangs vinnslunnar.

Viðskiptavinur ber ábyrgð á að upplýsa OR um breytingar sem gera þarf á upplýsingum um hann.

10. Öryggi persónuupplýsinga um viðskiptavini

OR tryggir öryggi persónuupplýsinga með tæknilegum og skipulagslegum ráðstöfunum. Um þær ráðstafanir er fjallað nánar í upplýsingaöryggisstefnu OR og viðeigandi leiðbeiningaskjölum í rekstrarhandbók OR.

Aðgangur að persónuupplýsingum um viðskiptavini er takmarkaður við þá starfsmenn, sem nauðsynlega þurfa slíkan aðgang til að ná fram tilgangi vinnslunnar. Starfsmenn eru upplýstir og meðvitaðir um skyldu þeirra til að viðhalda trúnaði og öryggi persónuupplýsinga sem þeir hafa aðgang að. Trúnaður og þagnarskylda þeirra gildir áfram þótt látið sé af störfum.

Að öðru leyti en kveðið er á um hér að framan fer um meðferð persónuupplýsinga um starfsmenn skv. lögum nr. 90/2018 um persónuvernd og vinnslu persónuupplýsinga, og ráðstöfunum sem innleiddar eru af hálfu OR á grundvelli þeirra.

Persónuverndarfulltrúi OR er Hörður Helgi Helgason, lögmaður á Landslögum, Borgartúni 26, 105 Reykjavík, sími 520-2900, personuverndarfulltrui@or.is.

3

Orkuveita Reykjavíkur

Ráðstafanirnar

- innleiddar á grundvelli stefnunnar

- Rekstrarhandbók uppfærð
  - Aðgangsréttur einstaklinga tryggður
    - Leiðbeiningar
    - Eyðublað v. beiðni um upplýsingar um vinnslu og eftir atvikum um aðgang að gögnum er tengjast vinnslu persónuupplýsinga.
  - Leiðbeiningar og verklag vegna meðferðar brota á vernd persónuupplýsinga (öryggisbrestur)
  - Leiðbeiningar og verklag við gerðs MÁP - mat á áhrifum á persónuvernd
  - Uppfærsla ýmissa annarra skjala í rekstrarhandbók til að tryggja hlítingu
    - T.d. vegna rafrænnar vöktunar
      - Tetra stöðvar; Símtalsupptökur í þjónustuveri; Ökuritar; Gæslumyndavélar

Orkuveita Reykjavíkur

Ráðstafanirnar (frh.)

- Sértækt á sviði starfsmannamála
  - Ráðningarsamningar uppfærðir
    - Upplýsingagjöf um persónuvernd og vinnslu upplýsinga færð þar inn
  - Innra vefsvæði uppfært
    - Persónuverndarstefna og greinargerð ásamt tilvísunum í helstu skjöl
  - Verkferlar og leiðbeiningar uppfærðar
    - T.d. um upplýsingagjöf við þjálfun nýrra starfsmanna
  - Breytingar gerðar á upplýsingagjöf og meðferð umsókna um störf
  - Sérstök áhersla m.t.t. viðkvæmra upplýsinga um starfsmenn
    - Vinnslusamningar
    - Dulkóðun í póstsendingum eftir atvikum

- ON Hlöður – sértækir skilmálar uppfærðir vegna samþykkis
  - https://www.on.is/greinargerd-til-vidskiptavina-vegna-vinnslu-upplysinga-a-grundvelli-samthykkis

Orkuveita Reykjavíkur

UM OR

SAGA OR

STARFSEMI

- Dótturfélög
- Gildi
- Gæðastefna
- Staðlar og gæðavottun
- Persónuverndarstefna

SKIPULAG OG STJÓRNENDUR

STJÓRNHÆTTIR

VINNUSTAÐURINN

FJÖLMIÐLAR

Persónuverndarstefna

Öll meðferð Orkuveitu Reykjavíkur (OR) á persónuupplýsingum lýtur lögum um persónuvernd og vinnslu persónuupplýsinga og reglum sem settar eru samkvæmt þeim. OR gætir þess að öll vinnsla persónuupplýsinga innan fyrirtækisins sé í samræmi við framangreind lög og tryggir að vinnsluaðilar sem fá aðgang að persónuupplýsingum fylgi þeim einnig.

OR upplýsir einstaklinga um þá vinnslu persónuupplýsinga sem á sér stað á vegum fyrirtækisins og í hvaða tilgangi hún er unnin. OR tryggir að vinnsla fari ekki fram í öðrum tilgangi en upplýst hefur verið um nema með fullri vitneskju og eftir atvikum með samþykki hlutaðeigandi.

Einstaklingar geta óskað upplýsinga um vinnslu sem á sér stað hjá OR og varðar þá sjálfa. Þeir geta andmælt henni telji þeir að hún samræmist ekki gildandi lögum og reglum og eftir atvikum krafist þess að röngum, villandi eða ófullkomnum persónuupplýsingum um sig verði eytt.

Greinargerð um vinnslu OR á persónuupplýsingum

Beiðni um upplýsingar

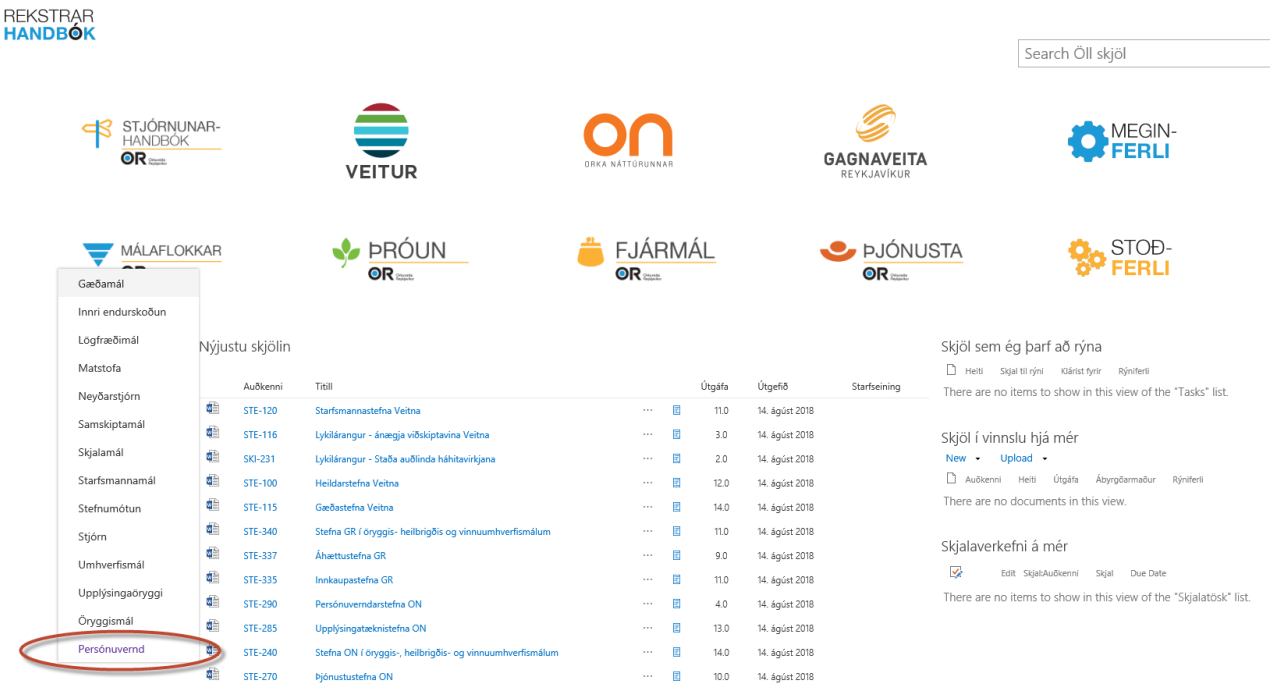
Samkvæmt lögum um persónuvernd og vinnslu persónuupplýsinga eiga einstaklingar rétt á að fá staðfestingu á því frá OR og dótturfélögum hvort verið sé að vinna persónuupplýsingar um þá og, ef svo er, hafa þeir rétt til aðgangs að persónuupplýsingunum og að fá nánari upplýsingar um tiltekin atriði sem tengjast vinnslunni.

Ef þú vilt fá aðgang að gögnum á grundvelli laga um persónuvernd, þá biðjum við þig að fylla út þar til gert eyðublað. Útfyllt eyðublað sendirðu í tölvupósti á netfangið beidniumupplysingar@or.is. Við afgreiðum beiðnina þína svo fljótt sem verða má.

Beiðni um upplýsingar á grundvelli persónuverndarlaga

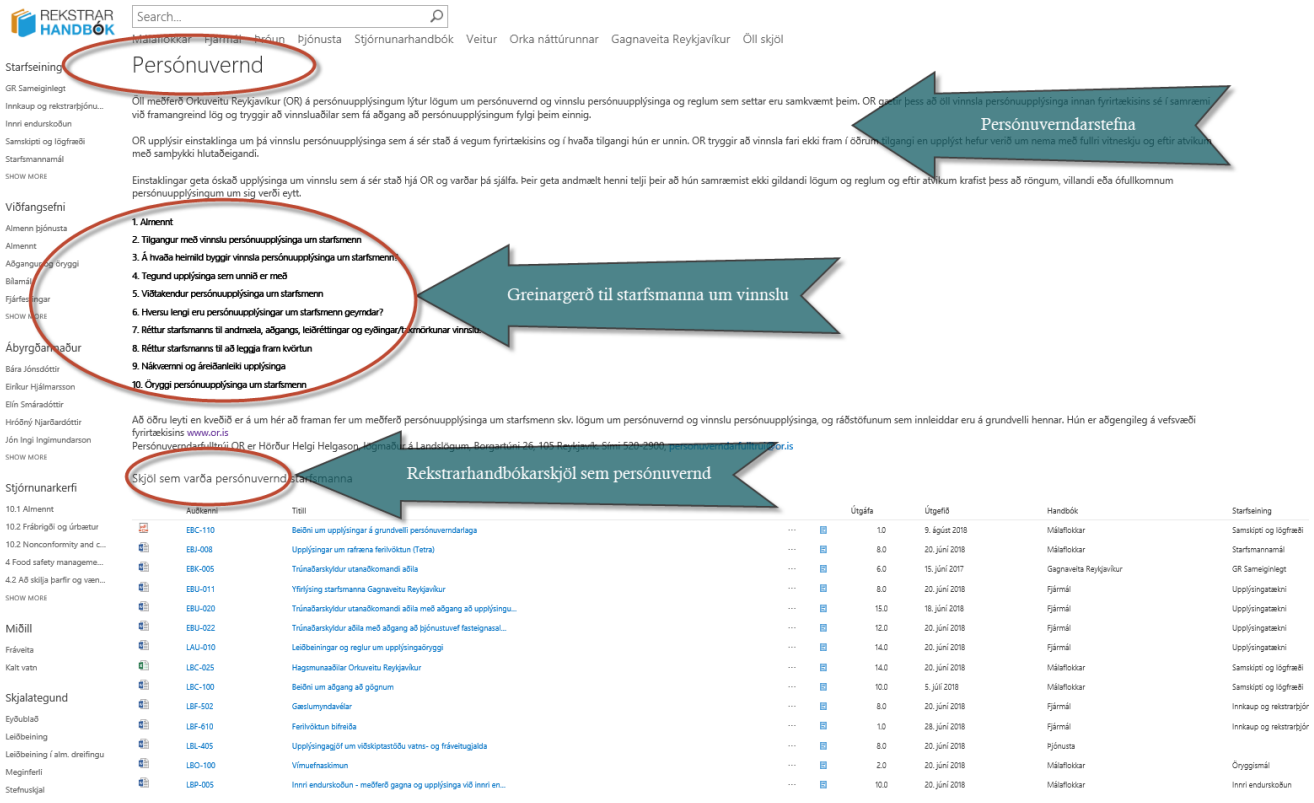
Nýtt svæði í rekstrarhandbók

- Málaflokkar OR: Persónuvernd



Orkuveita Reykjavíkur

Persónuverndarsvæði í rekstrarhandbók



Orkuveita Reykjavíkur

Áskorun við innleiðingu

- OR er skila- og vistunarskyldur aðili
  - Eyðing eingöngu heimil á grundvelli heimilda frá Borgarskjalaverði
  - Mikilvægt að rýna reglulega upplýsingar sem unnið er með
    - Með það að leiðarljósi að takmarka vinnsluna við það sem er nauðsynlegt hverju sinni
    - Einnig til að taka afstöðu til þess hvort óska eigi heimildar til að eyða gögnum
  - Aðgangur takmarkaður að upplýsingum þegar verkefni er lokið eða vinnu með þær er lokið

Orkuveita Reykjavíkur

Mat á persónuvernd er sífelluverkefni

- Á döfinni
  - Rýni og eftir atvikum gerð / uppfærsla vinnslusamninga
  - Rýni og eftir atvikum uppfærsla þjónustusamninga samstæðu
  - Yfirferð yfir upplýsingavinnslu m.t.t. grisjunar og eða breytts verklags til að lágmarka vinnslu
  - Úttektir og rýni til að tryggja áframhaldandi hlítingu
- Hvernig tryggjum við hlítingu?
  - Innri úttektir skjala skv. úttektaráætlun að lágmarki á 3ja ára fresti
  - Í upphafi þó ári eftir gildistöku nýs skjals
    - Verður viðhaft um öll skjöl sem viðkoma persónuvernd
  - Fræðsla til starfsmanna með reglubundnum hætti
    - Námskeið 1x á ári um lög og reglur þ.m.t. PVRG

Orkuveita Reykjavíkur

Orkuveita Reykjavíkur

HAGSÝNI FRAMSÝNI HEIÐARLEIKI