KPMG

Ert bú klár?

Ný persónuverndarlöggjöf

Fimm skref til að hagnýta regluverkið

Ert þú klár?

Mestu breytingar sem gerðar hafa verið á lögum um persónuvernd í yfir 20 ár munu taka gildi í maí 2018, með sektarákvæðum allt upp að 20 milljónir evra eða 4 prósent af rekstrartekjum eftir því hvort er hærra. Þess má vænta að eftirlitsaðilar muni beita þessum nýju ákvæðum til verndar hagsmunum einstaklinga.

Hinar nýju samevrópsku persónuverndarreglur (e. General Data Protection Regulation – GDPR) fela hins vegar ekki aðeins í sér ógn, heldur einnig tækifæri. Í nútíma viðskiptaumhverfi eru persónuupplýsingar verðmæti og viðskiptalegur hvati, og vönduð stefna í meðferð getur skapað fyrirtækjum umtalsvert samkeppnisforskot.

Hvernig geta nýjar reglur skapað forskot?
Rétt er að hafa í huga að persónuupplýsingar geta verið ein af helstu auðlindum fyrirtækja.

Af því leiðir að allir ferlar sem snerta persónuupplýsingar fela í sér tækifæri. Tækifæri til að fá betri skilning á þörfum viðskiptavina og bæta frammistöðu fyrirtækja á markaði með því að halda utan um og auka gæði persónuupplýsinga.

Það þarf gott skipulag og vandaða stefnu til að tryggja að slík gögn séu áreiðanleg, viðskiptavinir skilji til hvers þau eru notuð og geti gefið upplýst samþykki fyrir notkun þeirra. Þetta tryggir að hægt sé að draga hagnýtar ályktanir af gögnunum, gerir kleift að bjóða sérsniðna vöru eða þjónustu og dregur úr líkum á því að viðskiptavinir upplifi gagnasöfnun með neikvæðum hætti.

Fimm skref til að uppfylla kröfurnar

Byggt á víðtækri reynslu KPMG af þjónustu á sviði persónuverndar í mörgum löndum og í ólíkum atvinnugreinum, leggur KPMG til eftirfarandi fimm skrefa nálgun. Þessa nálgun má nýta bæði til að mæta kröfum regluverksins eða sem víðtækari nálgun við persónu- og gagnavernd.

1. Skilgreina stefnu um meðferð persónuupplýsinga

Hver er ásættanleg áhætta í vernd persónuupplýsinga hjá fyrirtækinu? Hvar vill fyrirtækið vera í samanburði við sambærilega aðila? Hvað í nýju löggjöfinni skiptir mestu máli fyrir fyrirtækið og viðskiptavini þess? Hver ber ábyrgð á yfirstjórn persónuverndarmála hjá fyrirtækinu?

Fyrsta skrefið er að skilgreina stefnu um meðferð persónuupplýsinga. Án slíkrar stefnu er ekki hægt að nálgast verkefnið með markvissum hætti. Stefnan þarf að vera skýr og markmiðadrifin, og hafa fullan stuðning frá yfirstjórn. Verkefnið þarf að komast á dagskrá stjórnar fyrirtækisins sem fyrst. Reynsla okkar er sú að flest fyrirtæki þurfi að ráðast í umbótaverkefni til að bæta meðferð persónuupplýsinga.

2. Greina núverandi stöðu

Nauðsynlegt er að greina núverandi stöðu fyrirtækisins til að átta sig á umfangi og áherslum í verkefninu sem fram undan er. Ekki nægir að fara yfir einfaldan gátlista heldur þarf að fara með skipulögðum hætti yfir rekstrarumhverfið og greina hvar og með hvaða hætti regluverkið snertir gögn og rekstur fyrirtækisins.

Í þessum tveimur fyrstu skrefum þarf að hafa í huga hvaða þættir regluverksins, og gagnaverndar almennt, eru lykilþættir fyrir fyrirtækið. Hvað er það sem skiptir mestu máli?

- **Hlíting og regluverk** – útfæra atburða-skráningu (e. audit trail) sem sýnir fram á að tæknilegum kröfum sé mætt.
- **Markaðssókn –** ná tökum á meðferð persónuupplýsinga svo hægt sé að koma nýjum vörum hratt á markað og skapa sérstöðu.
- **Aukið gagnamagn –** með nýrri tækni, svo sem interneti hlutanna (IoT) og gervigreind er að verða sprenging í gagnamagni sem skapar auknar áskoranir í persónuverndarmálum.
- **Alþjóðavæðing** – með auknum gagnaflutningi heimshorna á milli, á sama tíma og ný löggjöf um persónuvernd tekur gildi í æ fleiri löndum, þarf að tryggja að ekki sé óafvitandi brotið gegn reglum.
- **Útvistun** – gríðarlegur vöxtur í notkun tölvuskýja, útvistun og gagnahýsingu skapar nýjar áskoranir sem takast þarf á við.
- **Gögn viðskiptavina**– viðskiptavinum mun í auknum mæli standa til boða að færa gögn sín á milli þjónustuaðila, og því verður einfaldara að færa viðskiptin til samkeppnisaðila. Þetta skapar nýjar ógnir fyrir fyrirtæki sem eru ekki með sín mál í lagi.
- **Orðspor** – það nægir að horfa til nýlegra gagnaleka og tölvuárása til að sjá þann skaða sem slík atvik geta valdið orðspori fyrirtækja.

3. Gera þarf raunhæfa aðgerðaráætlun

Setja þarf saman raunhæfa áætlun um aðgerðir til að ná utan um áhættuþætti í samræmi við stefnu fyrirtækisins. Það þýðir ekki endilega að stefnt sé að því að vera í fremstu röð í öllum þáttum – heldur að hafa skýra sýn á hvar fyrirtækið vill vera.

Hvar á að byrja? Það veltur á því hver ásættanleg áhætta er fyrir fyrirtækið, en hér eru nokkrir þætti sem mætti huga að:

- **Stjórnskipulag, gagnasöfn og áhættur** – þessir þættir tengjast. Það þarf að greina hvaða gagnasöfn eru til staðar, hvernig halda á utan um þau og hvaða áhættur tengjast þeim svo hægt sé að meta ásættanlega stöðu og innleiða viðeigandi eftirlitsþætti til samræmis.
- **Réttur einstaklingsins –** réttur einstaklinga til að láta eyða gögnum eða „rétturinn til að gleymast“ og krafa um varðveislu gagna geta skarast. Ef ekki er skýrt hvaða gögnum er safnað eða hvort gögnum er safnað umfram það sem nauðsynlegt er, getur verið erfitt að mæta þeim kröfum. Aðgengi að eigin gögnum verður einstaklingum að kostnaðarlausu svo búast má við verulegri aukningu á fyrirspurnum, og fyrirtæki hafa aðeins mánuð til að afgreiða slíkar beiðnir.
- **Ferlar vegna frávika –** nýtt og krefjandi ákvæði er um að öll öryggisfrávik séu tilkynnt eftirlitsaðilum innan 72 klukkustunda. Það þarf skýra og góða ferla til að geta brugðist við, greint og upplýst innan þess tímaramma.
- **Samningar og verklag þjónustuaðila** – fyrirtæki þurfa að öðlast skilning á hvernig þjónustuaðilar þeirra útfæra sín persónuverndarmál. Í þjónustusamningum þurfa að vera skýr ákvæði um meðferð slíkra gagna, skilgreinda tímalengd á varðveislu og heimildir til eftirlits með framkvæmdinni. Vinnsluaðilar þurfa að mæta sambærilegu regluverki um gagnavernd og ábyrgðaraðilar.
- **Fræðsla–** tryggja þarf að starfsfólk sé meðvitað um áhrif regluverksins og hafi skilning á því með hvaða hætti það snertir þau og þeirra starf. Allt starfsfólk mun þurfa á grunnfræðslu að halda en þar sem mikið er unnið með persónuupplýsingar, svo sem í mannauðs- og markaðsdeildum, þarf markvissa fræðslu.
- **Úttekt á þjónustuaðilum –** mörg fyrirtæki hafa aukið eftirlit með sínum þjónustuaðilum á undanförnum árum, en fæstir ná þó að mæta þeim kröfum sem nýtt regluverk kveður á um. Yfirfara þarf samninga við þjónustuaðila og tryggja að þeir séu í samræmi við nýjar kröfur og koma á reglubundnu eftirliti með þjónustu þeirra.

4. Samræma aðgerðir og hrinda í framkvæmd

Innleiða þarf viðeigandi verklag við daglegan rekstur og leggja áherslu á þau svið þar sem áhættan er mest, en það krefst samræmingar þvert á fyrirtækið. Tryggja þarf aðkomu viðeigandi aðila svo sem lögfræði-, upplýsingatækni, mannauðs- og markaðssviðs og að nægur mannafli sé tiltækur í verkefnið. Vanmetið ekki verkefnið – persónuupplýsingar eru út um allt í fyrirtækinu.

5. Fella inn í daglegan rekstur

Aðlögun að nýja regluverkinu snýst um að skilgreina, innleiða og viðhalda viðeigandi ferlum. Frá og með árinu 2018 munu fyrirtæki reglulega þurfa að sýna fram á með hvaða hætti persónuupplýsinga er aflað, þær nýttar, varðveittar, afhentar og þær grisjaðar með hliðsjón af gildandi lögum og reglum sem og ákvæðum um persónuvernd. Það mun hafa áhrif á alla þá þætti er varða meðferð persónuupplýsinga og kalla á miklar breytingar innan fyrirtækja á næstunni.

Í stuttu máli, þá þarf regluverið og grundvallaratriði þess um ábyrga meðferð persónuupplýsinga að verða hluti af daglegum rekstri fyrirtækja og stofnana. Sýna þarf fram á með hvaða hætti þessum grundvallaratriðum er fylgt svo sem með því að skjalfesta hvernig ákvarðanir er teknar um vinnslu gagna og geta sýnt fram á að meginreglu sé fylgt.

Hvernig er hægt að sýna fram á ábyrga meðferð gagna? Það þarf meðal annars að:

- Skjalfesta framkvæmd áhættumats
- Viðhalda yfirliti yfir gagnasöfn
- Skilgreina og skýra hlutverk og ábyrgð á persónuverndarmálum
- Skjalfesta stefnu um meðferð persónuupplýsinga, verklag og ferla
- Skilning á því hvernig þjónustuaðilar vinna með útvistuð gögn
- Innleiðingu á viðurkenndum stjórnkerfum, svo sem ISO 27001

Með því að ná utan um og viðhalda ábyrgri stjórn á meðhöndlun gagna verður vinnslan skilvirkari og skapar aukið virði umfram það að uppfylla regluverkið. Fyrirtækið getur þannig að mætt ákvæðum laga um meðferð persónuupplýsinga og eflt stöðu sína á markaði.

Af hverju?

Okkar verkferlar eru í góðu lagi
Það er sjaldnast raunin, en jafnvel þó að núverandi verkferlar mæti vel ákvæðum eldri reglna eru verulegar líkur á að gera þurfi aðlaganir til að þeir uppfylli ákvæði nýrrar löggjafar.

Við erum sátt við að gera bara nóg til að þetta „sleppi til“
Þetta er varhugaverð nálgun því eftirlitsaðilar eiga eftir að setja skýrari línur um ýmis atriði. Það er hægt að taka ákvörðun um að eyða ekki gömlum upplýsingum eða skrám um viðskiptavini, en er ætlunin að halda áfram að nálgast viðskiptavini með vörur og þjónustu án þeirra samþykki? Þetta eru ákvarðanir sem samkvæmt regluverkinu þurfa að vera skjalaðar og teknar af stjórnendum fyrirtækisins. Jafnvel þó það sé gert, er óvíst að ákvörðun um að taka slíka áhættu, án þess að geta sýnt fram á að aðrar leiðir hafi verið kannaðar, yrði talin ásættanleg af hálfu eftirlitsaðila.

Við erum með fulla stjórn á persónuverndarmálum hjá okkur
Umfang gagna sem verða til innan fyrirtækja er gríðarlegt – frá mannauðsmálum til söludeilda, markaðsmálum til fjármálasviðs. Það er mikil áskorun að koma á samræmdri, skilvirkri og áhrifaríkri nálgun við persónuverndarmál – og krefst kröftugs stuðnings og eftirfylgni af hálfu yfirstjórnar.

KPMG er skýr valkostur

Við höfum á að skipa þverfaglegu teymi reyndra sérfræðinga á sviði persónuverndarmála

Við búum yfir reynslu af því að greina, hanna og innleiða stjórnskipulag persónuverndar á fjölmörgum sviðum.

Nýttu þér hagnýta og raunhæfa nálgun okkar byggt á alþjóðlegri reynslu

Hafðu samband

Davíð Kr. Halldórsson

Partner
dhalldorsson@kpmg.is

Soffía Eydís Björgvinsdóttir

Partner
sbjorgvinsdottir@kpmg.is

Ingi Tómasson

Verkefnastjóri
itomasson@kpmg.is

Hrafnkell Óskarsson

Verkefnastjóri
hoskarsson@kpmg.is

Download on the App Store