

Lai gan sods par jaunās regulas neievērošanu fiziskām personām nedraud, tomēr katra spēkos ir rīkoties, lai pasargātu savus personas datus un kontrolētu, kam tie tiek nodoti, stāsta zvērinātu advokātu biroja Sorainen advokāts un partneris Agris Repšs.

Trešdien, 28.martā, Saeimas Juridiskā komisija 1. lasījumam virzīja Personas datu apstrādes likuma projektu, kas precizēs jaunās Vispārīgās datu aizsardzības regulas (GDPR) piemērošanu Latvijā. To ir vērts zināt, kā uzņēmējiem, tā iedzīvotājiem.

Kad prasa personas datus, iedziļinieties - kāpēc?

“Mēs ikdienā nepievēršam uzmanību, ka mums prasa nodot personas datus, kad aizpildām pieteikumus mobilā telefona lietotnēm, sociālo tīklu profiliem vai kādu pakalpojumu saņemšanai. Taču faktiski uzņēmumi bieži vāc un apstrādā personas datus dažādām vajadzībām, piemēram, tās izmanto, lai piedāvātu labāku pakalpojumu, veidotu efektīvākas mārketinga kampaņas, kā arī ir gadījumi, kad, pārdodot datus, tiek gūti papildu ienākumi. Tāpēc mūsu datu aizsardzība visupirms, ir mūsu pašu rokās” skaidro Repšs.

Piemēram, reizēm, sūtot iespējamajam darbadevējam savu CV, cilvēki aiz ieraduma sniedz vairāk personiskas informācijas nekā nepieciešams - visbiežāk personas kodu, ģimenes stāvokli un informāciju par bērniem, arī foto attēlu.

“Pret saviem personas datiem jāizturas ar atbildību. Jāpārdomā, kādu informāciju par sevi padarām publiski pieejamu vai nododam citu personu un uzņēmumu rīcībā. Reizēm der sev uzdot jautājumu, vai prasītā informācija tik tiešām ir nepieciešama, lai saņemtu pakalpojumu,” uzsvēra Repšs.

Pirms nodot kādam uzņēmumam savus personas datus, ir vērts iepazīties ar tā personas datu apstrādes noteikumiem. Šī informācija visbiežāk būs atrodamā līgumu nosacījumos vai privātuma politiku aprakstošos dokumentos.

“Līdz ar jaunās regulas stāšanos spēkā ikvienam būs tiesības pieprasīt uzņēmumam sniegt informāciju par to, kādi personas dati ir tā rīcībā, kā un kādiem mērķiem tos izmanto, kā arī lūgt tos labot vai dzēst,” uzsvēra Repšs.

Jāņem vērā, ka personas datu apstrādei ne vienmēr ir nepieciešama īpaša personas piekrišana. Personas datus bez tās drīkst apstrādāt, ja šāds pienākums uzlikts ar likumu, ja tiek veikti uzdevumi sabiedrības interesēs, tie nepieciešami līguma izpildei vai ja pastāv leģitīmas intereses, piemēram, persona ir uzņēmuma darbinieks. Tomēr katrā no šiem gadījumiem, datu apstrādei ir jābūt samērīgai un iemeslam pamatotam. Pārbaudiet savu digitālo saimniecību

“Veiciet savu mazo personīgo datu auditu! Kādās vietnēs esat reģistrējies, kādu informāciju par sevi esat norādījis, mobilo telefonu un sociālo tīklu lietotņu gadījumā, kādai informācijai esat atļāvuši piekļuvi. Ja vietni vai lietotni izmantojat regulāri, pārbaudiet vai, norādītā informācija ir aktuāla, izdzēsiet lieko. Ja piemirsies kādās vietnēs esat reģistrējies, pārskatiet e-pastu, lietotnes mobilajā telefonā, varat arī savu vārdu ievadīt interneta pārlūka meklētājā, tur noteikti atradīsiet vismaz vienu vietni, kurā esat reģistrējušies un par kuru būsiat piemirsuši,” iesaka IT uzņēmuma Squalio pārstāvis Mareks Gruškevics.

Squalio pārstāvis aicina pārliecināties, vai datoram un viedtālrunim ir uzstādītas antivīrusa programmas, kā arī lejupielādēt programmu atjauninājumus, jo tie nereti ietver dažādus drošības uzlabojumus.

“Drošība vienmēr ir atkarīga no vājākā ķēdes posma. Slēgtas durvis nebūs šķērslis zaglim, kuram ir atslēga, un durvju atslēga šajā gadījumā ir jūsu parole,” uzskata Gruškevics.

Lai parole būtu iespējami drošāka, jāņem vērā pāris vienkārši padomi. Veidojot paroles, izvēlieties sarežģītākas burtu un ciparu kombinācijas. Ģimenes locekļa vai mājdzīvnieka vārds noteikti nebūs labākā izvēle. Ja sarežģītās paroles ir grūti izdomāt un paturēt prātā, izmantojiet lietotnes, kas ģenerē un šifrē paroles. Centieties katrai vietnei un lietotnei izmantot citu paroli. Citādāk, ja uzņēmumā, kurā glabājas jūsu dati, notiks datu noplūde (piemēram, uzlauzta lietotāju datu bāze), bet jūs vienu un to pašu paroli izmantojat arī citur, uzbrucējs itin viegli varēs iegūt piekļuvi visai jūsu digitālajai saimniecībai.

Ja vietne šādu iespēju piedāvā, noteikti izmantojiet divpakāpju verifikāciju. Tas nozīmē, ka ievadot paroli jums prasīs ievadīt papildu informāciju, piemēram, izziņā nosūtītu kodu. Līdzīgi kā interneta bankā jūs ievadiet lietotāja vārdu, paroli un ciparu kombināciju no kodu kalkulatora.

Galū galā, jūsu datu drošība ir saistīta arī ar tik vienkāršiem paradumiem, kā neglabāt lietotāja vārdus un paroles acīmredzamās vietās un, strādājot ar datoru publiskās vietās, pārliecināties, ka jums aiz muguras neviens nestāv un nelūkojas monitorā, iesaka speciālists.

Kas ir personas dati?

Atgādinām, ka personas dati ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu. Šāda informācija ir vārds, uzvārds, telefona numurs, e-pasta adrese, dzīvesvietas adrese, automašīnas reģistrācijas numurs, etniskā izcelsme, politiskie uzskati, reliģiskā pārliecība, bankas konta numurs, informācija par veselības stāvokli, biometriskie dati, informācija par ģimenes locekļiem, personas kods, attēls, paraksts un cita tamlīdzīga informācija.

Kāpēc ir nepieciešamas pārmaiņas?

Likumīgums, godprātība un pārredzamība - pamatprincipi, kas jāievēro glabājot un apstrādājot personas datus. Eiropas iedzīvotāji uzskata, ka viņu personas dati nav aizsargāti. Piemēram, deviņi no desmit Eiropas iedzīvotājiem ir izteikuši bažas, ka mobilās

lietotnes vāc datus bez viņu piekrišanas, bet septiņi no desmit uztrauc viņu datu iespējamā izmantošana. Pašreizējais regulējums nenovērš visus riskus, kas varētu rasties vācot, glabājot un apstrādājot personas datus.

Jaunā regula dod iespēju katram cilvēkam līdz visiem sīkumiem uzzināt, kādus datus par viņu uzņēmums glabā, kādiem mērķiem un cik ilgi izmanto, vai tie ir drošībā, kā arī kam un ar kādu mērķi tie var tikt nodoti. Cilvēkam ir tiesības kontrolēt, kā viņa personas dati tiek izmantoti, aizliegt tos izmantot vai pat pieprasīt dzēst no datubāzēm.

Kādas vēl personai ir tiesības?

Tiesības tikt aizmirstam (datu dzēšana) - Eiropas Savienības pilsoņiem būs tiesības pieprasīt pārtraukt personas datu apstrādi un datus dzēst. Ja kāds ir devis piekrišanu personas datu apstrādei ar noteiktu mērķi (atspoguļot sociālajos tīklos), bet ir pārdomājies, šādā gadījumā vairs nav pamata datus uzglabāt. Piemēram, bērni (neapzinoties iespējamās sekas) padarījuši datus publiski pieejamus. Jaunā kārtība ļaus izvairīties no

šādas rīcības sekām.

Datu pārnesamības tiesības (Data portability) - uzņēmumiem, pēc pašas personas pieprasījuma, ir pienākums izsniegt viņu rīcībā esošo datu elektronisku kopiju.

Piekrišana datu apstrādei - sniedzot piekrišanu personas datu apstrādei, tai jābūt izteiktai apstiprinošā formā vai ar skaidrām, aktīvām darbībām; lietotājam jābūt iespējai atsaukt piekrišanu bez iespējama kaitējuma sev. Tiesības pieprasīt, lai lēmumus, kuru pamatā ir automatizēta datu apstrāde, pieņemtu cilvēks, nevis mākslīgā intelekta sistēma.

Bērnu datu apstrāde - piekrišanu bērna personas datu apstrādei var sniegt vecāki (vai likumiskie pārstāvji).

Personas datu apstrādes likuma projektā bērniem paredzētas tiesības jau no 13 gadu vecuma sniegt piekrišanu saņemt informācijas sabiedrības pakalpojumus - piemēram reģistrēties sociālajos tīklos, saņemt komerciāla rakstura paziņojumus.

Atgādinām, 2018.gada 25.maijā Eiropā stāsies spēkā jaunie personas datu apstrādes noteikumi Vispārīgā personas datu aizsardzības regula. Jaunie noteikumi attieksies uz katru personu, kuras dati tiek vākti un apstrādāti, kā arī iepriekš savāktiem datiem.

ZAB Sorainen un IT uzņēmums Squalio ir apvienojuši kompetences un izveidojuši produktu "GDPR Ready", kas ietver neatkarīgu juridisko un IT sistēmu auditu, profesionālus ieteikumus nepieciešamajām izmaiņām, lai uzņēmums būtu gatavs GDPR.

<https://www.diena.lv/raksts/latvija/zinas/es-datu-aizsardzibas-regula-padomi-parastam-cilvekam-14194516>