



Latvijas Republikas tiesībsargs

Baznīcas iela 25, Rīga, LV-1010, tālr.: 67686768, e-pasts: tiesibsargs@tiesibsargs.lv, www.tiesibsargs.lv

Rīgā

09.09.2026 Nr. 1-5/186

Ministru kabinetam

Par preventīvu pasākumu veikšanu informācijas sistēmu drošības un personas datu aizsardzības nodrošināšanai

Īstenojot savu uzdevumu aizsargāt un veicināt cilvēktiesību ievērošanu, vēršu Ministru kabineta uzmanību uz nepieciešamību pastiprināti pievērsties personas datu aizsardzībai, informācijas sistēmu drošībai un ar personas datu apstrādi saistīto risku savlaicīgai identificēšanai un novēršanai. Minēto jautājumu nozīmīgumu atspoguļo vairākās informācijas sistēmās konstatētie informācijas drošības incidenti, kuru rezultātā ievērojams Latvijas iedzīvotāju personas datu apjoms nonāca trešo personu rīcībā. Neatkarīgi no konkrēto incidentu cēloņiem, to norise vēl vairāk apliecina, ka valsts pārvaldes rīcībā esošo datu aizsardzībai jābūt vienai no augstākajām prioritātēm.

Personas datu aizsardzība nav tikai tehnoloģiskās drošības jautājums. Tā ir personas tiesību uz privātās dzīves neaizskaramību sastāvdaļa un līdz ar to arī būtisks tiesiskas valsts elements. Saskaņā ar Latvijas Republikas Satversmes (turpmāk – Satversme) 96. pantu ikvienam ir tiesības uz privātās dzīves, mājokļa un korespondences neaizskaramību. Šīs pamattiesības starptautiskajos cilvēktiesību dokumentos formulētas līdzīgi¹, paredzot, ka personas datus ir jāapstrādā godprātīgi, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos. Turklāt no minētajiem regulējumiem izriet, ka neviena privātajā dzīvē nedrīkst patvarīgi vai nelikumīgi iejaukties. Kā atzinusi Satversmes tiesa, tiesības uz privātās dzīves neaizskaramību nozīmē, ka indivīdam ir tiesības uz savu privāto telpu, iespējams minimāli ciešot no valsts vai citu personu iejaukšanās.²

¹ Eiropas Cilvēka tiesību un pamatbrīvību aizsardzības konvencijas 8. pants, Eiropas Savienības Pamattiesību hartas 7. un 8. pants, Līguma par Eiropas Savienības darbību 16. panta 1. punkts, ANO Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām 17. pants, ANO Vispārējās cilvēktiesību deklarācijas 12. pants.

² Satversmes tiesas 2009. gada 23. aprīļa spriedums lietā Nr. 2008-42-01, 8. un 9. punkts un 2019. gada 5. decembra spriedums lietā Nr. 2019-01-01, 16.1. punkts.

Atbilstoši Satversmes tiesas praksē³ un zinātniskajā literatūrā⁴ paustajām atziņām valstij ir pienākums veikt Satversmes 96. pantā ietverto pamattiesību nodrošināšanai nepieciešamās darbības. Tas nozīmē, ka valstij nepieciešams pieņemt tādus likumus, kas pietiekami garantē personas tiesības uz datu aizsardzību no pretlikumīgas izmantošanas gan valsts pārvaldes, gan arī privāttiesību jomā. Taču minētā pienākuma īstenošana attiecas ne tikai izstrādājot un pieņemot normatīvo regulējumu par personas datu aizsardzību, bet arī uzraugot šā regulējuma īstenošanu praksē, tostarp regulāri pārliedzinoties par noteiktās kārtības un tehnoloģisko risinājumu uzlabošanas iespējām.

Ievērojot minēto, aicinu Ministru kabinetu izvērtēt, vai informācijas sistēmas, kuras plaši izmanto valsts un pašvaldību funkciju nodrošināšanai, izpilda visas nepieciešamās drošības prasības, identificēt esošās sistēmas riskus un pārliedzināties par to, ka personas dati tiek apstrādāti atbilstoši Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk – Regula) prasībām.

Būtiski, lai personas datu apstrāde atbilstu Regulas 5. pantā⁵ noteiktajiem personas datu apstrādes principiem, tostarp datu minimizēšanas un glabāšanas ierobežojuma principiem. Informācijas sistēmu pārziņiem nepieciešams pārliedzināties par to, ka tiek apstrādāti tikai tie personas dati, kas nepieciešami to apstrādes nolūkiem. Savukārt glabāšanas ierobežojuma princips mazina potenciālos riskus datu subjektam, pēc iespējas samazinot personas datu apstrādes laiku un pēc apstrādes personas datu dzēšot. Glabāšanas ierobežojuma principa būtība ir glabāt personas datus tikai tik ilgi, cik tas nepieciešams noteiktā personas datu apstrādes nolūka sasniegšanai.⁶ Ievērojot Eiropas Savienības Tiesas praksē secināto, jo ilgāk datus pārzinis glabā, jo lielāka ietekme uz datu subjekta interesēm un privāto dzīvi un jo augstākas ir prasības attiecībā uz šīs informācijas glabāšanas likumīgumu.⁷ Līdz ar to uzskatu, ka informācijas sistēmu drošības izvērtējumā nepieciešams pārliedzināties par to, ka personas datu apstrāde atbilst Regulas 5. pantā ietvertajiem personas datu apstrādes principiem.

³ Satversmes tiesas 2011. gada 20. oktobra spriedums lietā [Nr. 2010-72-01](#), 17.1. punkts.

⁴ Aut. kol. Baloža R. zin. red. (2011). Latvijas Republikas Satversmes komentāri. VIII nodaļa. Cilvēka pamattiesības. (247. lpp.). Latvijas Vēstnesis.

⁵ Eiropas Parlamenta un Padomes regula (ES) 2016/679 (2016. gada 27. aprīlis) [par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ direktīvu 95/46/EK \(Vispārīgā datu aizsardzības regula\)](#)

⁶ Aut. kol. Plepa J. un Ruķera M. zin. red. (2026). Vispārīgā datu aizsardzības regula. Skaidrojumi un komentāri (162. lpp.). Tiesu namu aģentūra.

⁷ Eiropas Savienības Tiesas 2023. gada 7. decembra spriedums [C-26/22 un C64/22 UF, AB v. Land Hessen](#), 95. punkts.

Īpaši vēlos uzsvērt, ka nepieciešams pārliecināties, vai veselības datu apstrāde E-veselība sistēmā un bērnu personas datu apstrāde E-klase sistēmā tiek nodrošināta atbilstošā apmērā, ievērojot datu minimizēšanas principu, un saskaņā ar drošības standartiem, kas novērš šo personas datu aizsardzības iespējamus pārkāpumus.

Veselības dati un bērnu personas dati pēc sava rakstura ir īpaši aizsargājami, jo to nepamatota, neatbilstošā vai nelikumīga apstrāde var radīt būtisku kaitējumu pacientu un bērnu tiesībām. Lai nodrošinātu veselības aprūpes organizēšanu un atvieglotu veselības aprūpes pakalpojumu sniegšanu, valsts ir noteikusi veselības informācijas sistēmas pārzini – sabiedrību ar ierobežotu atbildību "Latvijas Digitālās veselības centrs".⁸ Savukārt izglītības nozarē valsts ir noteikusi obligāto dokumentāciju, kas ir nepieciešama vispārējās izglītības iestāžu pedagoģiskā procesa organizācijai, tostarp izglītības iestādes noteikts dokuments informācijas apmaiņai ar vecāku, pilngadīgo izglītojamo vai atbildīgo amatpersonu.⁹ Šā dokumenta saturu un formu nosaka izglītības iestādes vadītājs, tāpēc izglītības iestāde dokumentāciju var nodrošināt elektroniski, izmantojot E-klase sistēmu vai citu sistēmu. Piemēram, bērnu personas datus E-klase sistēmā tehniski apstrādā SIA "Izglītības sistēmas". Ļaujot privāto tiesību juridiskām personām apstrādāt šos īpaši aizsargājamus personu datus, uzskatu, ka valstij ir rūpīgi un regulāri jāpārbauda šīs apstrādes atbilstību Regulas un drošības prasībām.

Ņemot vērā minēto, aicinu Ministru kabinetu izvērtēt, vai valsts un pašvaldību iestādes preventīvi nodrošina to pārziņā esošo informācijas sistēmu drošību, īstenoto personas datu apstrādes, tehnisko un organizatorisko pasākumu atbilstību Regulas prasībām.

Ar cieņu

tiesībsardze

Karina Palkova

⁸ [Ārstniecības likums](#), 78. pants un Ministru kabineta 2014. gada 11. marta noteikumi Nr. 134 "[Noteikumi par vienoto veselības nozares elektronisko informācijas sistēmu](#)", 2.punkts.

⁹ [Vispārējās izglītības likums](#), 4. panta 17. punkts un Ministru kabineta 2021. gada 10. augusta noteikumi Nr. 528 "[Vispārējās izglītības iestāžu un profesionālās izglītības iestāžu pedagoģiskā procesa un eksaminācijas centru profesionālās kvalifikācijas ieguves organizēšanai obligāti nepieciešamā dokumentācija](#)", 2.12. apakšpunkts.