

Kādas datu aizsardzības prasības jāievēro politiskajām partijām? 3/35/22

Attiecībā uz fizisko personu datu apstrādi, politiskās partijas nav nekāds izņēmums, un tām šo datu apstrādē jāievēro tās pašas Vispārīgās datu aizsardzības regulas (VDAR) prasības, kas noteiktas jebkuram citam datu pārzinim. Zīmīgi, ka Datu valsts inspekcija nesen publicējusi jaunas vadlīnijas par fizisko personu datu apstrādi priekšvēlēšanu laikā. Vai tas varētu liecināt, ka uzraudzības iestāde pastiprināti vērtēs partiju atbilstību VDAR prasībām? Šajā rakstā – par to, kādi pasākumi veicami partijai, lai nodrošinātu VDAR atbilstošu datu apstrādi.

Ieskatoties politisko partiju oficiālajās mājaslapās, var secināt, ka teju katrā ir nepilnības un neatbilstības (nav sniegta informācija par VDAR noteikto datu subjektu tiesību nodrošināšanu, sīkdatnes tiek apstrādātas bez tiesiskā pamata u.c.). Tā kā daudzu politisko partiju kandidāti un biedri nāk no uzņēmējdarbības vides, vēlamies atgādināt par vairākām būtiskām lietām, kas partijām jāņem vērā, apstrādājot fizisko personu datus priekšvēlēšanu laikā.

Vai ir atbilstošs privātuma paziņojums?

Partijas mājaslapā publicētajā privātuma paziņojumā jānorāda VDAR 13. un 14. pantā noteiktās datu subjektu tiesības, kā arī jāspēj tās izpildīt, ja datu subjekts to pieprasa. Tas vien, ka ir izstrādāts privātuma paziņojums, vēl nenozīmē, ka tas atbilst VDAR prasībām, tāpēc jāpievērš uzmanība, lai paziņojums ir viegli saprotams, pārskatāms un paredzēts konkrētai mērķauditorijai, kā arī ir skaidri aprakstīti datu apstrādes mērķi.

Vai datu apstrādei ir tiesisks pamats?

Katram datu apstrādes mērķim ir nepieciešams tiesisks pamats, kam jābūt arī norādītam privātuma paziņojumā. Tas vien, ka paziņojums kategoriski apgalvo, ka partijas veiktā personas datu apstrāde ir likumīga, vēl nenozīmē, ka tai ir tiesisks pamats. Tiesiskā pamata noteikšanā partijai jābūt īpaši rūpīgai, to detalizēti skaidrojot savā privātuma paziņojumā (piemēram, identificējama vēlētajā uzrunāšana, informācijas sniegšana KNAB par biedru naudas iemaksu, sīkdatņu apstrāde partijas mājaslapā, iegūto personas datu glabāšana mākonī). Katrai datu apstrādes darbībai jānosaka atbilstošākais datu apstrādes tiesiskais pamats.

Vai ir saņemta atbilstoša datu subjekta piekrišana?

Datu subjekta piekrišanai jābūt brīvai, konkrētai un nepārprotamai, to nedrīkst iekļaut veidlapu tekstos. Nav arī pareizi piekrišanas ķekšus ietvert jau iepriekš atzīmētos laukos – piekrišanas ķeksi par konkrēto datu apstrādes darbību atzīmē pats datu subjekts. Nekādā gadījumā uz vēlētajū nedrīkst izdarīt spiedienu, lai tas dalītos ar saviem datiem, piemēram, piezvanot vai sazinoties ar identificējamu personu sociālajos tīklos un lūdzot tai sniegt savus datus (e-pastu, adresi vai tālruņa numuru), lai turpmāk nosūtītu tai komerciālus paziņojumus. Tas nozīmē, ka nav atļauts uzrunāt datu subjektu, ja partija pirms tam nav saņēmusi no tā skaidru un nepārprotamu piekrišanu, ka persona vēlas tikt uzrunāta par konkrēto piedāvājumu.

Profilēšana, politiskā reklāma un aģitācija

Nereti partijas iegūst personas datus no trešajām personām, piemēram, starpniekiem, lai nosūtītu ziņojumus konkrētajai auditorijai vēlēšanu vai kampaņas mērķu sasniegšanai. Datus par politisko

pārlicību var izsecināt arī no dažādos avotos esošu personas datu analīzes pat tad, ja šie dati nav saistīti ar politiku, bet vērtējot personas uzvedību vai veicot citus novērojumus (piemēram, bildes, komentāri, ieraksti sociālajos tīklos). Partijai par šādu starpnieku datu izmantošanu ir pienākums informēt datu subjektu, norādot informāciju privātuma paziņojumā atbilstoši VDAR 14. pantam. Tāpat svarīgi, lai pirms šādu starpnieku datu izmantošanas partija veic pārbaudi ar mērķi pārlicināties, ka dati iegūti likumīgi.

Ja partija veic profilēšanu, tad arī par šo datu apstrādes darbību datu subjekts jāinformē privātuma paziņojumā un jāspēj izpildīt subjekta pieprasījums, ja tas vēlas atteikties no profilēšanas.

Vai ir ieviesti atbilstoši tehniskie risinājumi un organizatoriskie pasākumi?

Lai gan VDAR ļauj datu pārzinim noteikt, kādus pasākumus vai risinājumus tas ieviesīs, lai nodrošinātu VDAR atbilstošu datu apstrādi, šī atļauja tomēr būtiski neatvieglo pārziņa darbu, jo tam pašam jāvērtē, vai partijas veiktā datu apstrāde ir droša un atbilstoša un vai īstenotie pasākumi ir pietiekami. Turklāt partijai jāspēj uzskatāmi pierādīt, ka tā ir ieviesusi atbilstošus tehniskos risinājumus, izstrādājusi atbilstošu dokumentāciju un apmācījusi savus biedrus.

Pirms ārpakalpojuma izmantošanas partijai jāspēj noteikt, vai tā ietvaros jāslēdz datu apstrādes līgums. Nosūtot datus ārpus ES/EEZ, partijai jāvērtē, kādas garantijas tā ieviesīs, lai nodrošinātu VDAR atbilstību.

Atgādinām, ka partijām ir arī pienākums ievērot pārskatatbildības (*accountability*) principu, no kura izriet divi pamatpienākumi: pienākums nodrošināt VDAR prasību ievērošanu un spēja to pierādīt. Tas nozīmē, ka pārziņa pienākums ir rakstveidā dokumentēt visus ar datu aizsardzību saistītos noteikumus un lēmumus.

Diemžēl nav vienota saraksta ar izstrādājamiem datu aizsardzības dokumentiem, kas pierādītu VDAR prasību ievērošanu. Tādēļ partijām jāvērtē, vai tām ir pietiekamas zināšanas par datu aizsardzību, vai netiek veiktas tādas apstrādes darbības, kam piemērojams VDAR 37. pants par obligātu datu aizsardzības speciālista norīkošanu vai apstrādes darbību reģistrēšanu, un vai nav pienākums izstrādāt specifiskus datu aizsardzības dokumentus, kas izriet no VDAR noteikumiem.

Ņemot vērā iepriekš minēto, ja partijai rodas šaubas vai jautājumi par tās veikto personas datu apstrādi, aicinām konsultēties ar datu aizsardzības speciālistiem.