Տվյալների սուբյեկտի իրավունքների վերաբերյալ 01/2022 ուղեցույց. հասանելիության իրավունք[1]

Տարբերակ 2.0

Ընդունվել է 2023 թվականի մարտի 28-ին

[1] Սույն թարգմանությունը Տվյալների պաշտպանության եվրոպական խորհուրդի կողմից իրականացված պաշտոնական թարգմանություն չէ: Թարգմանությունն իրականացվել է Գերմանական միջազգային համագործակցության ընկերության (GIZ) ֆինանսական աջակցությամբ Արևելյան գործընկերության տարածաշրջանային ֆոնդի շրջանակներում: Թարգմանությունն իրականացվել է Անձնական տվյալների պաշտպանության, Գերմանական միջազգային համագործակցության ընկերության և Տվյալների պաշտպանության եվրոպական խորհուրդի միջև սերտ համագործակցության արդյունքում:

Տարբերակի պատմությունը

Տարբերակ 1.0	2022 թվականի հունվարի 18	Ուղեցույցի ընդունում՝ հանրային քննարկումների համար
Տարբերակ 2.0	2023 թվականի մարտի 28	Ուղեցույցի ընդունում՝ հանրային քննարկումներից հետո

Ամփոփ նկարագիրը

Տվյալների սուբյեկտների հասանելիություն ունենալու իրավունքն ամրագրված է Հիմնարար իրավունքների ԵՄ խարտիայի 8-րդ հոդվածում: Այն ի սկզբանե եղել է Տվյալների պաշտպանության եվրոպական իրավական շրջանակի մի մասը և ներկայումս էլ ավելի է կատարելագործվել ՏՊԸԿ 15-րդ հոդվածով սահմանված առավել հստակ և ճշգրիտ կանոններով:

Հասանելիություն ունենալու իրավունքի նպատակը և ընդհանուր կառուցվածքը

Հասանելիություն ունենալու իրավունքի ընդհանուր նպատակն է՝ անձանց տրամադրել իրենց անձնական տվյալների մշակման վերաբերյալ բավարար, թափանցիկ և հեշտ հասանելի տեղեկություններ, որպեսզի նրանք կարողանան տեղեկանալ իրենց տվյալների մշակման մասին և ստուգել դրա օրինականությունն ու մշակված տվյալների ճշգրտությունը: Սա կօգնի անձին հեշտությամբ իրացնել մյուս իրավունքները, ինչպես օրինակ՝ տվյալները ոչնչացնելու կամ ուղղելու իրավունքը, սակայն չի հանդիսանում այդ իրավունքների իրացման նախապայման:

Տվյալների պաշտպանության մասին օրենքի համաձայն՝ հասանելիություն ունենալու իրավունքը պետք է տարբերվի այլ նպատակներ հետապնդող համանման իրավունքներից, օրինակ՝ պաշտոնական փաստաթղթերին հասանելիություն ունենալու իրավունքից, որի նպատակն է երաշխավորել պետական մարմինների որոշումների կայացման գործընթացի թափանցիկությունը և վարչական լավագույն գործելակերպերի կիրառումը:

Այնուամենայնիվ, տվյալների սուբյեկտը պարտավոր չէ հիմնավորել հասանելիություն ստանալու մասին դիմումը, և հսկողի լիազորությունը չէ վերլուծել, թե արդյոք դիմումն իրականում կօգնի տվյալների սուբյեկտին ստուգել տվյալների համապատասխան մշակման օրինականությունը կամ իրացնել այլ իրավունքներ: Հսկողը պետք է ընթացք տա դիմումին, բացառությամբ եթե չպարզվի, որ դիմումը ներկայացվել է տվյալների պաշտպանության կանոններից տարբերվող՝ այլ կանոնների համաձայն:

Հասանելիություն ունենալու իրավունքը ներառում է երեք տարբեր բաղադրիչներ՝

- հաստատում, թե արդյոք անձի վերաբերյալ տվյալները մշակվում են, թե ոչ.
- այդ անձնական տվյալներին հասանելիություն և
- մշակման մասին տեղեկություններին հասանելիություն, այսինքն՝ մշակման նպատակը, տվյալների ու ստացողների կատեգորիաները, տևողությունը, տվյալների սուբյեկտների իրավունքները և երրորդ երկիր տվյալների փոխանցումների դեպքում՝ համապատասխան երաշխիքները:

Տվյալների սուբյեկտի դիմումը գնահատելու առնչությամբ ընդհանուր նկատառումները

Դիմումի բովանդակությունը վերլուծելիս հսկողը պետք է գնահատի, թե արդյոք դիմումը վերաբերում է դիմում ներկայացնող անձի անձնական տվյալներին, արդյոք դիմումը կարգավորվում է 15-րդ հոդվածով և արդյոք կան այլ, առավել կոնկրետ դրույթներ, որոնք կարգավորում են հասանելիությունը որոշակի ոլորտում: Նա պետք է նաև գնահատի, թե արդյոք դիմումը վերաբերում է տվյալների սուբյեկտի վերաբերյալ մշակված բոլոր

տվյալներին, թե միայն դրանց մի մասին:

Դիմումի ձևաչափի վերաբերյալ հատուկ պահանջներ գոյություն չունեն: Հսկողը պետք է ապահովի պատշաճ և հեշտ կիրառելի հաղորդակցման ուղիներ, որոնք հեշտությամբ կարող են օգտագործվել տվյալների սուբյեկտի կողմից: Այնուամենայնիվ, տվյալների սուբյեկտը կարող է չօգտագործել այդ հատուկ ուղիները, փոխարենը կարող է դիմումն ուղարկել հսկողի կապի ապահովման պաշտոնական կենտրոնին: Հսկողը պարտավոր չէ ընթացք տալ լրիվ պատահական կամ ակնհայտորեն սխալ հասցեներով ուղարկված դիմումներին:

Եթե հսկողը չի կարող նույնականացնել տվյալների սուբյեկտին վերաբերվող տվյալները, ապա նա պետք է այդ մասին տեղեկացնի տվյալների սուբյեկտին և կարող է մերժել հասանելիության ապահովումը, քանի դեռ տվյալների սուբյեկտը չի տրամադրել լրացուցիչ տեղեկություններ, որոնք հնարավոր են դարձնում տվյալների նույնականացումը: Ավելին, եթե հսկողը կասկածներ ունի տվյալների սուբյեկտի ինքնության առնչությամբ, ապա նա կարող է պահանջել լրացուցիչ տեղեկություններ՝ տվյալների սուբյեկտի ինքնությունը հաստատելու համար: Լրացուցիչ տեղեկությունների տրամադրման պահանջը պետք է համաչափ լինի մշակվող տվյալների տեսակին, այն վնասին, որը կարող է հասցվել և այլն՝ տվյալների սահմանազանցող հավաքագրումից խուսափելու համար:

Հասանելիություն ունենալու իրավունքի շրջանակը

Հասանելիություն ունենալու իրավունքի շրջանակը որոշվում է ՏՊԸԿ 4(1) հոդվածով սահմանված՝ անձնական տվյալների հասկացության շրջանակով: Հիմնական անձնական տվյալներից՝ անունից, հասցեից, հեռախոսահամարից և այլնից բացի այս սահմանման մեջ կարող են մտնել տարատեսակ տվյալներ, ինչպիսիք են բժշկական եզրակացությունները, գնումների պատմությունը, վարկունակության ցուցանիշները, ակտիվության մատյանները, որոնումները և այլն: Կեղծանունացված անձնական տվյալները շարունակում են մնալ անձնական տվյալներ՝ ի տարբերություն անանունացված տվյալների: Հասանելիություն ունենալու իրավունքը վերաբերում է դիմում ներկայացրած անձին վերաբերող անձնական տվյալներին: Սա չպետք է մեկնաբանվի չափազանց սահմանափակ կերպով և կարող է ներառել տվյալներ, որոնք կարող են վերաբերել այլ անձանց նույնպես, օրինակ՝ մուտքային և ելքային հաղորդագրությունները ներառող հաղորդակցության պատմությունը:

Անձնական տվյալներին հասանելիություն ապահովելուց բացի հսկողը պետք է լրացուցիչ տեղեկություններ տրամադրի տվյալների մշակման և տվյալների սուբյեկտների իրավունքների վերաբերյալ: Այդ տեղեկությունները կարող են հիմնված լինել հսկողի կողմից կազմված՝ տվյալների մշակման գործողությունների հաշվառման մատյանում առկա տեղեկությունների (ՏՊԸԿ 30-րդ հոդված) և գաղտնիության մասին ծանուցման վրա (ՏՊԸԿ 13-րդ և 14-րդ հոդվածներ): Այնուամենայնիվ, այս ընդհանուր տեղեկությունները կարելի է թարմացնել մինչև դիմումը ներկայացնելու պահը կամ հարմարեցնել՝ դիմում ներկայացրած կոնկրետ անձի առնչությամբ իրականացվող մշակման գործողություններն արտացոլելու համար:

Ինչպե՞ս ապահովել հասանելիությունը

Հասանելիություն ապահովելու ուղիները կարող են տարբեր լինել՝ կախված տվյալների քանակից և իրականացվող մշակման բարդությունից: Եթե այլ բան հստակորեն նշված չէ, ապա դիմումը պետք է ընկալվի որպես տվյալների սուբյեկտին վերաբերող *բոլոր* անձնական տվյալներին հասանելիություն ստանալու մասին դիմում, և հսկողը կարող է խնդրել տվյալների սուբյեկտին հստակեցնել դիմումը, եթե նա մշակում է մեծ քանակությամբ տվյալներ:

Հսկողը պետք է որոնի անձնական տվյալները բոլոր SS համակարգերում և SS-ի հետ առնչություն չունեցող հաշվառման համակարգերում՝ հիմնվելով տեղեկությունների համակարգվածության եղանակն արտացոլող որոնման չափանիշների, օրինակ՝ անվան և հաճախորդի համարի վրա: Տվյալների և մշակման վերաբերյալ այլ տեղեկությունների փոխանցումը պետք է իրականացվի հակիրճ, թափանցիկ, հասկանալի և հեշտ հասանելի ձևով՝ հստակ ու պարզ լեզվով: Այս առումով առավել ճշգրիտ պահանջների սահմանումը կախված է տվյալների մշակման հանգամանքներից, ինչպես նաև տվյալների սուբյեկտի՝ հաղորդակցությունն ընկալելու և ըմբռնելու կարողությունից (օրինակ՝ հաշվի առնելով, որ տվյալների սուբյեկտը երեխա է կամ հատուկ կարիքներ ունեցող անձ): Եթե տվյալները բաղկացած են ծածկագրերից կամ այլ «չմշակված տվյալներից», ապա դրանք պետք է բացատրվեն, որպեսզի տվյալների սուբյեկտի համար իմաստ արտահայտեն:

Հասանելիություն ապահովելու հիմնական եղանակը տվյալների սուբյեկտին իր տվյալների կրկնօրինակը տրամադրելն է, սակայն կարող են նախատեսվել այլ եղանակներ (օրինակ՝ բանավոր տեղեկություններ և տեղում հասանելիություն), եթե տվյալների սուբյեկտը դա պահանջի: Տվյալները կարող են ուղարկվել էլ. փոստի միջոցով՝ պայմանով, որ բոլոր անհրաժեշտ երաշխիքները կիրառված են՝ հաշվի առնելով, օրինակ՝ տվյալների բնույթը, կամ այլ եղանակով, օրինակ՝ ինքնասպասարկման գործիքի միջոցով:

Երբեմն, երբ առկա են մեծ քանակությամբ տվյալներ, և տվյալների սուբյեկտի համար դժվար կլինի ըմբռնել տեղեկությունները, եթե բոլոր տեղեկությունները տրամադրվեն մեկ խմբով, հատկապես առցանց եղանակով, ամենահարմար միջոցը կարող է լինել բազմաշերտ մոտեցման կիրառումը: Տարբեր շերտերով տեղեկությունների տրամադրումը կարող է դյուրացնել տվյալների սուբյեկտի կողմից տվյալների ըմբռնումը: Հսկողը պետք է կարողանա ապացուցել, որ բազմաշերտ մոտեցման կիրառումն ավելացված արժեք է ստեղծում տվյալների սուբյեկտի համար, և տեղեկությունները բոլոր շերտերով պետք է տրամադրվեն միաժամանակ, եթե այդպես է ցանկանում տվյալների սուբյեկտը:

Տվյալների կրկնօրինակը և լրացուցիչ տեղեկությունները պետք է տրամադրվեն ձևաչափի պահպանմամբ, օրինակ՝ գրավոր տեքստի ձևով, լայնորեն կիրառվող էլեկտրոնային եղանակով, որպեսզի տվյալների սուբյեկտը կարողանա այն հեշտությամբ ներբեռնել: Տվյալները կարող են տրամադրվել վերծանված կամ ամփոփ ձևով՝ պայմանով, որ բոլոր տեղեկությունները ներառված են, և դա չի փոխում տեղեկությունների բովանդակությունը:

Դիմումը պետք է կատարվի հնարավորինս արագ, սակայն ցանկացած դեպքում՝ այն ստանալուց հետո մեկ ամսվա ընթացքում: Հարկ եղած դեպքում այս ժամկետը կարող է երկարաձգվել ևս երկու ամսով՝ հաշվի առնելով դիմումի բարդությունն ու հերթական համարը: Այնուհետև տվյալների սուբյեկտը պետք է տեղեկացվի ձգձգման պատճառի մասին: Հսկողը պետք է ձեռնարկի անհրաժեշտ միջոցներ՝ դիմումներին հնարավորինս

արագ ընթացք տալու և այդ միջոցները տվյալների մշակման հանգամանքներին հարմարեցնելու համար: Եթե տվյալները պահպանվում են միայն շատ կարճ ժամանակահատվածով, ապա պետք է լինեն միջոցներ, որոնք կերաշխավորեն, որ հասանելիություն ստանալու մասին դիմումը կարող է, մինչև դրան ընթացք տալը, կատարվել առանց տվյալների ոչնչացման: Եթե մշակվում են մեծ քանակությամբ տվյալներ, ապա հսկողը պետք է գործադրի մշակման բարդությանը հարմարեցված ընթացակարգեր և մեխանիզմներ:

Դիմումի գնահատումը պետք է արտացոլի հսկողի կողմից դիմումն ստանալու պահին առկա իրավիճակը: Պետք է տրամադրվեն նույնիսկ այն տվյալները, որոնք կարող են սխալ լինել կամ մշակված լինել անօրինական ճանապարհով: Այն տվյալները, որոնք արդեն ջնջվել են, օրինակ՝ պահպանման քաղաքականությանը համապատասխան, և հետևաբար հսկողին այլևս հասանելի չեն, տրամադրվել չեն կարող:

Սահմաններն ու սահմանափակումները

ՏՊԸԿ-ով սահմանվում են հասանելիություն ունենալու իրավունքի որոշ սահմանափակումներ: Ոչ մի այլ բացառություն կամ շեղում նախատեսված չէ: Հասանելիություն ունենալու իրավունքից որևէ ընդհանուր վերապահում՝ կապված այն ջանքերի համաչափության հետ, որոնք հսկողը պետք է ձեռնարկի տվյալների սուբյեկտի դիմումը բավարարելու համար, չի կատարվում:

15(4) հոդվածի համաձայն՝ կրկնօրինակը ձեռք բերելու իրավունքը բացասաբար չի անդրադառնում այլ անձանց իրավունքների ու ազատությունների վրա: Տվյալների պաշտպանության եվրոպական խորհուրդը (այսուհետ՝ ՏՊԵԽ) գտնում է, որ այդ իրավունքները պետք է հաշվի առնվեն ոչ միայն կրկնօրինակը տրամադրելու միջոցով հասանելիություն ապահովելիս, այլ նաև այլ միջոցներով (օրինակ՝ տեղում հասանելիություն) տվյալներին հասանելիություն ապահովելու պարագայում: 15(4) հոդվածը, այնուամենայնիվ, կիրառելի չէ 15(1)«ա»-«ը» հոդվածով նշված՝ մշակման վերաբերյալ լրացուցիչ տեղեկությունների նկատմամբ: Հսկողը պետք է կարողանա ապացուցել, որ դա կոնկրետ իրավիճակում բացասաբար է անդրադառնում այլ անձանց իրավունքների կամ ազատությունների վրա: Ընդհանուր առմամբ 15(4) հոդվածի կիրառումը չպետք է հանգեցնի տվյալների սուբյեկտի դիմումի մերժման. դա միայն կհանգեցնի այն մասերը բացառելուն կամ անվերծանելի դարձնելուն, որոնք կարող են բացասաբար անդրադառնալ այլ անձանց իրավունքների ու ազատությունների վրա:

ՏՊԸԿ 12(5) հոդվածը թույլ է տալիս հսկողին մերժել ակնհայտորեն անհիմն կամ սահմանազանցող դիմումները, կամ այդ դիմումների համար գանձել ողջամիտ վճար: Այս հասկացություններին պետք է տալ նեղ մեկնաբանում: Քանի որ հասանելիություն ստանալու մասին դիմումների առնչությամբ գոյություն ունեն շատ քիչ նախապայմաններ, դիմումն ակնհայտորեն անհիմն դիտարկելու շրջանակը բավականին սահմանափակ է: Սահմանազանցող դիմումները պայմանավորված են այն ոլորտի առանձնահատկություններով, որտեղ գործունեություն է իրականացնում հսկողը: Որքան հաճախ են փոփոխություններ տեղի ունենում հսկողի տվյալների շտեմարանում, այնքան ավելի հաճախ կարող է տվյալների սուբյեկտը դիմել հասանելիություն ստանալու համար՝ այն չհամարելով սահմանազանցող: Հասանելիություն ունենալու ապահովումը մերժելու փոխարեն հսկողը կարող է որոշել տվյալների սուբյեկտից գանձել վճար: Սա

նպատակահարմար կլինի միայն սահմանազանցող դիմումներ ներկայացնելու դեպքում՝ այդ դիմումների ուսումնասիրության արդյունքում առաջացող վարչական ծախսերը ծածկելու համար: Հսկողը պետք է կարողանա ապացուցել դիմումի ակնհայտորեն անհիմն կամ սահմանազանցող լինելու հանգամանքը:

Հասանելիություն ունենալու իրավունքի սահմանափակումներ կարող են նախատեսված լինել նաև անդամ պետությունների ազգային իրավունքով՝ ՏՊՀԿ 23-րդ հոդվածի, ինչպես նաև դրանով սահմանված շեղումների համաձայն: Հսկողները, որոնք մտադիր են կիրառել այդ սահմանափակումները, պետք է մանրամասնորեն ուսումնասիրեն ազգային դրույթների պահանջները և հաշվի առնեն ցանկացած հատուկ պայման, որը կարող է կիրառվել: Այդ պայմաններից կարող են լինել հասանելիություն ունենալու իրավունքի իրացման միայն ժամանակավորապես հետաձգումը, կամ սահմանափակման կիրառումը միայն կոնկրետ կատեգորիայի տվյալների նկատմամբ:

Բովանդակություն

1 ՆԵՐԱԾՈՒԹՅՈՒՆ. ԸՆԴՀԱՆՈՒՐ ԴԻՏԱՐԿՈՒՄՆԵՐ 11

2 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՈՒՆԵՆԱԼՈՒ ԻՐԱՎՈՒՆՔԻ ՆՊԱՏԱԿԸ, ՏՊԸԿ 15-ՐԴ ՀՈԴՎԱԾԻ ԿԱՌՈՒՑՎԱԾՔԸ ԵՎ ԸՆԴՀԱՆՈՒՐ ՍԿԶԲՈՒՆՔՆԵՐԸ 14

2.1 Հասանելիություն ունենալու իրավունքի նպատակը 14

2.2 ՏՊԸԿ 15-րդ հոդվածի կառուցվածքը 16

2.2.1 Հասանելիություն ունենալու իրավունքի բովանդակության սահմանումը 17

2.2.1.1 Հաստատում, թե «արդյոք» անձնական տվյալները մշակվում են, թե ոչ 17

2.2.1.2 Մշակվող անձնական տվյալների հասանելիությունը 17

2.2.1.3 Մշակման և տվյալների սուբյեկտի իրավունքների մասին տեղեկությունները 18

2.2.2 Մեթոդների վերաբերյալ դրույթները 18

2.2.2.1 Կրկնօրինակի տրամադրումը 18

2.2.2.2 Լրացուցիչ կրկնօրինակներ տրամադրելը 20

2.2.2.3 Տեղեկությունները լայնորեն կիրառվող էլեկտրոնային եղանակով հասանելի դարձնելը .. 21

2.2.3 Հասանելիություն ունենալու իրավունքի հնարավոր սահմանափակումը 21

2.3 Հասանելիություն ունենալու իրավունքի ընդհանուր սկզբունքները 22

2.3.1 Տեղեկությունների ամբողջականությունը 22

2.3.2 Տեղեկությունների ճշգրտությունը 25

36. Տվյալների սուբյեկտին տրամադրված անձնական տվյալների օրինակում ներառված տեղեկությունները պետք է պարունակեն տվյալների սուբյեկտի մասին պահվող փաստացի տեղեկությունները կամ անձնական տվյալները: Սա ներառում է տեղեկությունների տրամադրման պարտավորություն այն տվյալների մասին, որոնք ճշգրիտ չեն կամ այն տվյալների մասին, որոնց մշակումն օրինական կամ այլևս օրինական չէ: Տվյալների սուբյեկտը կարող է, օրինակ՝ օգտվել հասանելիություն ունենալու իրավունքից՝ տարբեր հսկողների միջև շրջանառվող ոչ ճշգրիտ տվյալների աղբյուրը պարզելու համար: Եթե հսկողն ուղղել է ոչ ճշգրիտ տվյալները՝ մինչև տվյալների սուբյեկտին այդ մասին հայտնելը, ապա տվյալների սուբյեկտը զրկված կլինի այդ հնարավորությունից: Նույնը վերաբերում է անօրինական ճանապարհով մշակմանը: Տվյալների սուբյեկտին վերաբերող տվյալների՝ անօրինական ճանապարհով մշակման մասին տեղեկանալու հնարավորությունը հասանելիություն ունենալու իրավունքի հիմնական նպատակներից մեկն է: Մշակման անփոփոխ վիճակի մասին տեղեկացնելու պարտավորությունը չի հակասում հսկողի՝ անօրինական ճանապարհով մշակումը դադարեցնելու կամ ոչ ճշգրիտ տվյալներն ուղղելու պարտավորությանը: Այն հարցերի պատասխանները, թե ինչ հերթականությամբ պետք է կատարվեն այդ պարտավորությունները, ներկայացված են հետևյալ բաժնում: 25

2.3.3 Գնահատման ելակետային ժամանակը 25

2.3.4 Տվյալների անվտանգության պահանջների կատարումը 27
3 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՍՏԱՆԱԼՈՒ ՄԱՍԻՆ ԴԻՄՈՒՄՆԵՐԻՆ ՎԵՐԱԲԵՐՈՂ ԸՆԴՀԱՆՈՒՐ ԴԻՏԱՐԿՈՒՄՆԵՐԸ 27
3.1 Ներածություն 27
3.1.1 Դիմումի բովանդակության վերլուծությունը 28
3.1.2 Դիմումի ձևը 31
3.2 Նույնականացումը և իսկորոշումը 33
3.3 Դիմում ներկայացնող անձի իսկորոշման համաչափության գնահատումը 36
3.4 Երրորդ անձանց/վստահված անձանց միջոցով ներկայացված դիմումները 40
3.4.1 Երեխաների անունից հասանելիություն ունենալու իրավունքի իրացումը 41
3.4.2 Երրորդ անձի կողմից տրամադրված պորտալների/ալիքների միջոցով հասանելիություն ունենալու իրավունքի իրացումը 42
4 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՈՒՆԵՆԱԼՈՒ ԻՐԱՎՈՒՆՔԻ ՇՐՋԱՆԱԿԸ ԵՎ ԱՅՆ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐՆ ՈՒ ՏԵՂԵԿՈՒԹՅՈՒՆՆԵՐԸ, ՈՐՈՆՑ ԴԱ ՎԵՐԱԲԵՐՈՒՄ Է 43
4.1 Անձնական տվյալների սահմանումը 43
4.2 Անձնական տվյալները, որոնց վերաբերում է հասանելիություն ունենալու իրավունքը 49
4.2.1 «Իրեն վերաբերող անձնական տվյալներ» 49
4.2.2 «Մշակվող» անձնական տվյալները 52
4.2.3 Հասանելիություն ստանալու մասին նոր դիմումի շրջանակը 53
4.3 Մշակման և տվյալների սուբյեկտի իրավունքների վերաբերյալ տեղեկությունները 53
5 ԻՆՉՊԵ՞Ս ԿԱՐՈՂ Է ՀՍԿՈՂՆ ԱՊԱՀՈՎԵԼ ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ 59
5.1 Ինչպե՞ս կարող է հսկողն առբերել պահանջվող տվյալները 60
5.2 Հասանելիություն ապահովելու համար համապատասխան միջոցները 61
5.2.1 «Համապատասխան միջոցներ» ձեռնարկելը 61
5.2.2 Հասանելիություն ապահովելու տարբեր միջոցները 62
5.2.3 «Հակիրճ, թափանցիկ, հասկանալի և հեշտ հասանելի ձևով՝ պարզ ու հասարակ լեզվով» հասանելիություն ապահովելը 65
5.2.4 Մեծ քանակությամբ տեղեկությունները պահանջում են տեղեկությունների տրամադրման եղանակների նկատմամբ հատուկ պահանջներ 67
5.2.5 Զևաչափը 70
5.3 Հասանելիություն ապահովելու ժամկետները 73
6 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՈՒՆԵՆԱԼՈՒ ԻՐԱՎՈՒՆՔԻ ՍԱՀՄԱՆՆԵՐՆ ՈՒ ՍԱՀՄԱՆԱՓԱԿՈՒՄՆԵՐԸ 75
6.1 Ընդհանուր դիտարկումները 75
6.2 ՏՊԸԿ 15(4) հոդվածը 76

6.3 ՏՊԸԿ 12(5) հոդվածը 80
6.3.1 Ի՞նչ է նշանակում ակնհայտորեն անհիմն 80
6.3.2 Ի՞նչ է նշանակում սահմանազանցող 81
6.3.3 Հետևանքները 85
6.4 ՏՊԸԿ 23-րդ հոդվածի հիման վրա Միության կամ անդամ պետությունների իրավունքով նախատեսված հնարավոր սահմանափակումները և շեղումները 86
ՀԱՎԵԼՎԱԾ. ԳԾԱՊԱՏԿԵՐ 87

Տվյալների պաշտպանության եվրոպական խորհուրդը

Հաշվի առնելով «Անձնական տվյալների մշակման մասով ֆիզիկական անձանց պաշտպանության և այդ տվյալների ազատ տեղաշարժի, ինչպես նաև 95/46/ԵՀ հրահանգը (այսուհետ՝ Տվյալների պաշտպանության ընդհանուր կանոնակարգ) ուժը կորցրած ճանաչելու մասին» Եվրոպական պառլամենտի և Խորհրդի 2016 թվականի ապրիլի 27-ի 2016/679/ԵՄ կանոնակարգի 70 (1)(ե) հոդվածը,

հաշվի առնելով ԵՏՏ համաձայնագիրը և, մասնավորապես, դրա XI հավելվածը և 37-րդ արձանագրությունը, որը փոփոխվել է ԵՏՏ համատեղ կոմիտեի 2018 թվականի հուլիսի 6-ի թիվ 154/2018 որոշմամբ[1],

հաշվի առնելով դրա Աշխատակարգի 12-րդ և 22-րդ հոդվածները,

քանի որ այս ուղեցույցի նախապատրաստական աշխատանքների շրջանակներում հավաքվում էին շահագրգիռ կողմերի կարծիքներն ինչպես գրավոր կերպով, այնպես էլ տվյալների սուբյեկտի իրավունքների վերաբերյալ շահագրգիռ կողմերի հատուկ միջոցառման ժամանակ՝ ՏՊԸԿ համապատասխան դրույթների կիրառման հետ կապված մարտահրավերներն ու մեկնաբանման խնդիրները վերհանելու համար.

ԸՆԴՈՒՆԵՑ ՀԵՏԵՎՅԱԼ ՈՒՂԵՑՈՒՅՑԸ

1 ՆԵՐԱԾՈՒԹՅՈՒՆ. ԸՆԴՀԱՆՈՒՐ ԴԻՏԱՐԿՈՒՄՆԵՐ

1. Ժամանակակից հասարակությունում անձնական տվյալները մշակվում են պետական և մասնավոր սուբյեկտների կողմից բազմաթիվ գործողությունների ժամանակ, ամենատարբեր նպատակներով և զանազան եղանակներով: Անձինք կարող են հաճախ հայտնվել անբարենպաստ իրավիճակում՝ չհասկանալով, թե ինչպես են մշակվում, այդ թվում՝ կոնկրետ դեպքում ինչ տեխնոլոգիայով են մշակվում իրենց անձնական տվյալները, լինի դա մասնավոր, թե պետական սուբյեկտի կողմից: Այս իրավիճակներում ֆիզիկական անձանց անձնական տվյալները պաշտպանելու համար ՏՊԸԿ-ով նախատեսվել է ընդհանուր առմամբ տվյալների մշակման տարբեր տեսակների նկատմամբ կիրառելի համահունչ և ամուր իրավական դաշտ, այդ թվում՝ տվյալների սուբյեկտի իրավունքներին վերաբերող հատուկ դրույթներ:

2. Անձնական տվյալների հասանելիության իրավունքը ՏՊԸԿ III գլխով նախատեսված՝ տվյալների սուբյեկտների իրավունքներից մեկն է, ի թիվս այլ իրավունքների, ինչպիսիք են ուղղելու և ոչնչացնելու իրավունքը, մշակումը սահմանափակելու իրավունքը, տեղափոխելիության իրավունքը, տվյալները մշակելու դեմ առարկության իրավունքը կամ ավտոմատացված անհատական որոշումների կայացման, այդ թվում՝ պրոֆիլավորման ենթակա չլինելու իրավունքը[2]: Տվյալների սուբյեկտի հասանելիության իրավունքն ամրագրված է ինչպես Հիմնարար իրավունքների ԵՄ խարտիայում (Խարտիա)[3], այնպես էլ ՏՊԸԿ 15-րդ հոդվածում, որտեղ այն հստակ կերպով ձևակերպված է որպես անձնական տվյալներին և հարակից այլ տեղեկություններին հասանելիության իրավունք:

3. ՏՊԸԿ համաձայն՝ հասանելիության իրավունքը բաղկացած է երեք բաղադրիչից՝ հաստատում այն մասին, թե արդյոք անձնական տվյալները մշակվում են, թե ոչ, դրանց

հասանելիությունը և հենց մշակման գործընթացի վերաբերյալ տեղեկությունները: Տվյալների սուբյեկտը կարող է նաև ստանալ մշակված անձնական տվյալների կրկնօրինակը, մինչդեռ այդ հնարավորությունը տվյալների սուբյեկտի լրացուցիչ իրավունքը չէ, այլ տվյալներին հասանելիություն ապահովելու եղանակը: Այսպիսով, հասանելիության իրավունքը կարող է ընկալվել որպես տվյալների սուբյեկտի հնարավորություն՝ հարցնելու հսկողին, թե արդյոք իր վերաբերյալ անձնական տվյալները մշակվում են, թե ոչ, և որպես այդ տվյալներին հասանելիություն ստանալու ու դրանք ստուգելու հնարավորություն: Հսկողը տվյալների սուբյեկտին իր դիմումի հիման վրա տրամադրում է ՏՊԸԿ 15-րդ հոդվածի 1-ին և 2-րդ մասերով նախատեսված տեղեկությունները:

4. Հասանելիության իրավունքն իրացվում է ինչպես տվյալների պաշտպանության մասին օրենքի շրջանակներում՝ տվյալների պաշտպանության օրենքի նպատակներին համապատասխան, այնպես էլ ավելի կոնկրետ՝ ՏՊԸԿ 1(2) հոդվածով սահմանված՝ «*ֆիզիկական անձանց հիմնարար իրավունքների ու ազատությունների և մասնավորապես անձնական տվյալների պաշտպանության իրենց իրավունքի*» շրջանակներում: Հասանելիության իրավունքը համարվում է տվյալների պաշտպանության ամբողջ համակարգի կարևոր տարր:

5. Հասանելիության իրավունքի գործնական նպատակն է՝ հնարավորություն ընձեռել ֆիզիկական անձանց հսկողություն իրականացնելու իրենց անձնական տվյալների նկատմամբ[4]: Այս նպատակը գործնականում արդյունավետորեն իրականացնելու համար ՏՊԸԿ-ն նպատակ ունի դյուրացնել դրա իրականացումը մի շարք երաշխիքների միջոցով, որոնք տվյալների սուբյեկտին ընձեռում են այդ իրավունքը հեշտությամբ իրացնելու հնարավորություն՝ առանց անհարկի սահմանափակումների, ողջամիտ պարբերականությամբ և առանց ավելորդ ձգձգումների կամ ծախսերի: Այս ամենը պետք է հանգեցնի թվային դարաշրջանում տվյալների սուբյեկտի կողմից հասանելիության իրավունքի առավել արդյունավետ իրացմանը, որի մի մասն է կազմում նաև առավել լայն իմաստով տվյալների սուբյեկտի՝ վերահսկող մարմին բողոք ներկայացնելու իրավունքը և արդյունավետ դատական պաշտպանության իրավունքը:[5]

6. Ինչ վերաբերում է հասանելիության իրավունքի զարգացմանը՝ որպես տվյալների պաշտպանության իրավական շրջանակի մաս, հարկ է ընդգծել, որ այն ի սկզբանե եղել է տվյալների պաշտպանության եվրոպական համակարգի տարր: Ի հակադրություն 95/46/ԵՀ հրահանգի՝ ՏՊԸԿ-ով սահմանված՝ տվյալների սուբյեկտի իրավունքների ստանդարտը թե՛ լրամշակվել և թե՛ կատարելագործվել է. սա վերաբերում է նաև հասանելիության իրավունքին: Քանի որ հասանելիության իրավունքի իրացման մեթոդներն այժմ առավել ճշգրիտ ներկայացված են ՏՊԸԿ-ում, այս իրավունքը նաև իրավական որոշակիության տեսանկյունից առավել ուսուցողական է ինչպես տվյալների սուբյեկտի, այնպես էլ հսկողի համար: Բացի դրանից, ՏՊԸԿ 15-րդ հոդվածի հատուկ ձևակերպումը և դրա 12(3) հոդվածի համաձայն տվյալներ տրամադրելու հստակ վերջնաժամկետը պարտավորեցնում են հսկողին պատրաստ լինելու տվյալների սուբյեկտների հարցումներին՝ մշակելով դիմումներին ընթացք տալու ընթացակարգեր:

7. Հասանելիության իրավունքը չպետք է դիտարկել առանձին, քանի որ այն սերտորեն փոխկապված է ՏՊԸԿ այլ դրույթների, մասնավորապես՝ տվյալների պաշտպանության սկզբունքների հետ, այդ թվում՝ տվյալների մշակման արդարության ու օրինականության, հսկողի՝ թափանցիկություն ապահովելու պարտավորության և ՏՊԸԿ III գլխով

նախատեսված՝ տվյալների սուբյեկտի այլ իրավունքների հետ:

8. Տվյալների սուբյեկտի իրավունքների շրջանակներում կարևոր է նաև ընդգծել ՏՊԸԿ 12-րդ հոդվածի կարևորությունը, որով սահմանվում են ՏՊԸԿ 13-րդ և 14-րդ հոդվածներում նշված տեղեկությունների տրամադրման գործընթացում հսկողի կողմից ընդունված համապատասխան միջոցների և ՏՊԸԿ 15-22-րդ և 34-րդ հոդվածներում նշված հաղորդակցությունների նկատմամբ պահանջները. այդ պահանջները, ընդհանուր առմամբ, սահմանում են տվյալների սուբյեկտին և, մասնավորապես՝ երեխային ուղղված ցանկացած տեղեկությանը պատասխանելու ձևը, եղանակը և ժամկետը:

9. ՏՊԵԽ-ն անհրաժեշտ է համարում առավել ճշգրիտ կերպով ցույց տալ ուղղություն, թե ինչպես պետք է տարբեր իրավիճակներում կիրառվի հասանելիության իրավունքը: Այս ուղեցույցը նպատակ ունի վերլուծելու հասանելիության իրավունքի տարբեր հայեցակետերը: Առավել կոնկրետ՝ հաջորդ բաժնի նպատակն է ներկայացնել հենց 15-րդ հոդվածի ընդհանուր նկարագիրը և պարզաբանումը, մինչդեռ հաջորդող բաժիններում ներկայացվում է հասանելիության իրավունքի իրացման հետ կապված առավել հաճախ հանդիպող գործնական խնդիրների ու հարցերի առավել խորը վերլուծությունը:

---

[1] Սույն փաստաթղթում «անդամ պետություններին» կատարվող հղումները պետք է հասկանալ որպես «ԵՏՏ անդամ պետություններին» կատարվող հղումներ:

[2] ՏՊԸԿ 15-22-րդ հոդված:

[3] Հիմնարար իրավունքների Եվրոպական միության խարտիայի 8-րդ հոդվածի 1-ին կետի համաձայն՝ յուրաքանչյուր ոք ունի իրեն վերաբերող անձնական տվյալների պաշտպանության իրավունք: 8-րդ հոդվածի 2-րդ կետի 2-րդ նախադասության համաձայն՝ յուրաքանչյուր ոք ունի իրեն վերաբերող հավաքագրված տվյալներին հասանելիության և դրանք ուղղելու իրավունք:

[4] Տե՛ս ՏՊԸԿ 7-րդ, 68-րդ, 75-րդ և 85-րդ ներածական դրույթները:

[5] Տե՛ս ՏՊԸԿ VIII գլխի 77-րդ, 78-րդ և 79-րդ հոդվածները:

2 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՈՒՆԵՆԱԼՈՒ ԻՐԱՎՈՒՆՔԻ ՆՊԱՏԱԿԸ, ՏՊԸԿ 15-ՐԴ ՀՈԴՎԱԾԻ ԿԱՌՈՒՑՎԱԾՔԸ ԵՎ ԸՆԴՀԱՆՈՒՐ ՍԿԶԲՈՒՆՔՆԵՐԸ

2.1 Հասանելիություն ունենալու իրավունքի նպատակը

10. Այսպիսով, հասանելիություն ունենալու իրավունքը հնարավորություն է ընձեռում ֆիզիկական անձանց իրականացնել իրենց վերաբերող անձնական տվյալների նկատմամբ հսկողություն, քանի որ այն թույլ է տալիս նրանց «*տեղեկանալ մշակման մասին և ստուգել դրա օրինականությունը*»[6]: Ավելի կոնկրետ՝ հասանելիություն ունենալու իրավունքի նպատակն է հնարավորություն ընձեռել տվյալների սուբյեկտներին տեղեկանալու, թե ինչպես են մշակվում իրենց անձնական տվյալները, ինչպես նաև այդ մշակման հետևանքները, և ստուգել մշակված տվյալների ճշգրտությունը՝ առանց հիմնավորելու իրենց մտադրությունը: Այլ կերպ ասած՝ հասանելիություն ունենալու իրավունքի նպատակն է անձանց տրամադրել տվյալների մշակման վերաբերյալ բավարար, թափանցիկ և հեշտ հասանելի տեղեկություններ՝ անկախ օգտագործվող տեխնոլոգիաներից, ինչպես նաև նրանց հնարավորություն ընձեռել ստուգելու կոնկրետ մշակման գործողության տարբեր հայեցակետերը՝ ՏՊԸԿ համաձայն (օրինակ՝ օրինականությունը, ճշգրտությունը):

11. Սույն ուղեցույցներում ներկայացված՝ ՏՊԸԿ մեկնաբանումը հիմնված է մինչ այժմ ընդունված՝ ԵՄԱԴ-ի նախադեպային իրավունքի վրա: Հաշվի առնելով հասանելիություն ունենալու իրավունքի կարևորությունը՝ ակնկալվում է, որ հարակից նախադեպային իրավունքն ապագայում զգալիորեն կզարգանա:

12. ԵՄԱԴ-ի որոշումներին համապատասխան[7]՝ հասանելիություն ունենալու իրավունքը ծառայում է տվյալների սուբյեկտների անձեռնմխելիության և տվյալների պաշտպանության իրավունքը երաշխավորելուն[8] և կարող է նպաստել, օրինակ՝ ՏՊԸԿ 16-19-րդ, 21-22-րդ և 82-րդ հոդվածներից բխող իրավունքների իրացմանը: Այնուամենայնիվ, հասանելիություն ունենալու իրավունքի իրացումն անձի իրավունքն է և պայմանավորված չէ այդ մյուս իրավունքների իրացմամբ, և մյուս իրավունքների իրացումը կախված չէ հասանելիություն ունենալու իրավունքի իրացումից:

13. Հաշվի առնելով հասանելիություն ունենալու իրավունքի լայն նպատակը՝ նպատակահարմար չէ, որ հսկողը դրա նպատակը վերլուծի հասանելիություն ստանալու մասին դիմումների գնահատման շրջանակներում՝ որպես հասանելիություն ունենալու իրավունքի իրացման նախապայման: Այսպիսով, հսկողները չպետք է գնահատեն, թե «ինչու» է տվյալների սուբյեկտը պահանջում տվյալներին հասանելիություն, այլ միայն «ինչ» է նա պահանջում (տե՛ս դիմումի վերլուծության վերաբերյալ 3-րդ բաժինը), և արդյոք նրանք տիրապետում են տվյալ անձին վերաբերող անձնական տվյալների (տե՛ս 4-րդ բաժինը): Հետևաբար, օրինակ՝ հսկողը չպետք է մերժի հասանելիություն ապահովելն այն հիմքով կամ կասկածի հիման վրա, որ պահանջվող տվյալները տվյալների սուբյեկտի կողմից կարող են օգտագործվել՝ աշխատանքից ազատվելու կամ հսկողի հետ առևտրային վեճի դեպքում դատարանում իր պաշտպանությունն ապահովելու համար:[9] Հասանելիություն ունենալու իրավունքի սահմանների և սահմանափակումների

առնչությամբ տե՛ս 6-րդ բաժինը:

Օրինակ 1. Գործատուն աշխատանքից ազատել է աշխատողին: Մեկ շաբաթ անց վերջինս որոշում է ապացույցներ հավաքել՝ աշխատանքից անարդար ազատման հիմքով իր նախկին գործատուի դեմ հայց ներկայացնելու համար: Այս նպատակով աշխատողը գրում է նախկին գործատուին՝ խնդրելով իրեն՝ որպես տվյալների սուբյեկտ, տրամադրել իրեն վերաբերող բոլոր այն անձնական տվյալներին հասանելիություն, որոնք նախկին գործատուն՝ որպես հսկող, մշակում է:

Հսկողը չպիտի գնահատի տվյալների սուբյեկտի մտադրությունը, իսկ տվյալների սուբյեկտը պարտավոր չէ հսկողին ներկայացնել դիմումի պատճառը: Հետևաբար, եթե դիմումը բավարարում է բոլոր մյուս պահանջները (տե՛ս 3-րդ բաժինը), ապա հսկողը պետք է բավարարի դիմումը, բացառությամբ այն դեպքերի, երբ այն ակնհայտորեն անհիմն է կամ սահմանազանցող՝ ՏՊԸԿ 12(5) հոդվածին համապատասխան (տե՛ս 6.3 բաժինը), ինչը հսկողը պարտավոր է հիմնավորել:

Այլ տարբերակ. Տվյալների սուբյեկտը դատական գործընթացի ընթացքում իրացնում է իրեն վերաբերող անձնական տվյալներին հասանելիություն ունենալու իրավունքը: Այնուամենայնիվ, հսկողի և տվյալների սուբյեկտի միջև աշխատանքային հարաբերությունները կարգավորող՝ անդամ պետության ազգային իրավունքում առկա են որոշ դրույթներ, որոնք սահմանափակում են ընթացող կամ հետագա դատական գործընթացներում կողմերին տրամադրվելիք կամ նրանց միջև փոխանակվող տեղեկությունների շրջանակը, որոնք կիրառելի են տվյալների սուբյեկտի կողմից աշխատանքից անարդար ազատման հիմքով ներկայացված հայցին: Այս համատեքստում և պայմանով, որ այդ ազգային դրույթները համապատասխանում են ՏՊԸԿ 23-րդ հոդվածով[10] սահմանված պահանջներին, տվյալների սուբյեկտն իրավունք չունի հսկողից ստանալու ավելի շատ տեղեկություններ, քան նախատեսված է անդամ պետության՝ իրավական վեճերի կողմերի միջև տեղեկությունների փոխանակումը կարգավորող ազգային իրավունքի դրույթներով:

14. Թեև հասանելիություն ունենալու իրավունքն ունի լայն նպատակ, այնուամենայնիվ, ԵՄԱԴ-ը մեկնաբանել է նաև տվյալների պաշտպանության մասին օրենքի և հասանելիություն ունենալու իրավունքի գործողության սահմանները: Օրինակ՝ ԵՄԱԴ-ը գտել է, որ ԵՄ տվյալների պաշտպանության իրավունքով երաշխավորված հասանելիություն ունենալու իրավունքի նպատակը պետք է տարբերակվի ԵՄ և ազգային օրենսդրությամբ սահմանված՝ պաշտոնական փաստաթղթերի հասանելիություն ունենալու իրավունքի նպատակից, ընդ որում, ԵՄ և ազգային օրենսդրության նպատակն է «ապահովել պետական մարմինների որոշումների կայացման գործընթացի առավելագույն հնարավոր թափանցիկությունը և խթանել վարչական լավագույն գործելակերպերի կիրառումը»[11], նպատակ, որը չի հետապնդում տվյալների պաշտպանության մասին օրենքը: ԵՄԱԴ-ը եզրակացրել է, որ անձնական տվյալների հասանելիություն ունենալու իրավունքը կիրառվում է անկախ այն հանգամանքից, թե արդյոք հասանելիություն ունենալու այլ տեսակի իրավունքն այլ նպատակով, օրինակ՝ ուսումնասիրության ընթացակարգի համատեքստում, կիրառվում է, թե ոչ:

---

[6] ՏՊԸԿ 63-րդ ներածական դրույթ:

[7] ԵՄԱԴ, գործ թիվ C-434/16, *Նովակի* գործ [Nowak], ինչպես նաև թիվ C-141/12 և թիվ C-372/12 միացված գործեր, *Ուայէսը և այլք* գործ [YS and Others]:

[8] ԵՄԱԴ, գործ թիվ C-434/16, *Նովակի* գործ, պարբերություն 56:

[9] Այս թեմային առնչվող հարցերը հանդիսանում են ԵՄԱԴ-ում ներկայումս քննվող գործի քննության առարկա (C-307/22):

[10] ՏՊԸԿ 23-րդ հոդվածի համաձայն՝ Սահմանափակումների վերաբերյալ ՏՊԵԽ-ի 10/2020 ուղեցույց, հանրային քննարկումների համար նախատեսված տարբերակ, 2020 թվականի դեկտեմբերի 18:

[11] ԵՄԱԴ, թիվ C-141/12 և թիվ C-372/12 միացված գործեր, *Ուայէսը և այլք* գործ, պարբերություն 47:

2.2 ՏՊԸԿ 15-րդ հոդվածի կառուցվածքը

15. Հասանելիություն ստանալու մասին դիմումին պատասխանելու և դրա ոչ մի հարց չանտեսելու համար անհրաժեշտ է նախևառաջ հասկանալ 15-րդ հոդվածի կառուցվածքը և այդ հոդվածով նախատեսված հասանելիություն ունենալու իրավունքի մասը կազմող բաղադրիչները:

16. 15-րդ հոդվածը կարելի է բաժանել ութ տարբեր տարրերի՝ ստորև բերված աղյուսակում ներկայացված կարգով.

1.	Հաստատում, թե արդյոք հսկողը մշակում է դիմում ներկայացրած անձի անձնական տվյալները, թե ոչ	Հոդված 15(1), նախադասության առաջին կես
2.	Դիմում ներկայացրած անձին վերաբերող անձնական տվյալների հասանելիությունը	Հոդված 15(1), նախադասության երկրորդ կես (առաջին մաս)
3.	Մշակման վերաբերյալ հետևյալ տեղեկությունների հասանելիությունը՝ ա) մշակման նպատակները. բ) անձնական տվյալների կատեգորիաները. գ) ստացողները կամ ստացողների կատեգորիաները. դ) մշակման նախատեսվող տևողությունը կամ տևողությունը որոշելու չափանիշները. ե) տվյալներն ուղղելու, ոչնչացնելու, մշակումը սահմանափակելու և տվյալները մշակելու դեմ առարկության իրավունքի առկայությունը. զ) վերահսկող մարմին բողոք ներկայացնելու իրավունքը. է) ցանկացած հասանելի տեղեկություն տվյալների աղբյուրի վերաբերյալ, եթե հավաքագրված չէ տվյալների սուբյեկտից ը) ավտոմատացված որոշումների կայացումը, այդ թվում՝ պրոֆիլավորման և դրա հետ կապված այլ տեղեկությունների առկայությունը	Հոդված 15(1), նախադասության երկրորդ կես (երկրորդ մաս)
4.	46-րդ հոդվածի համաձայն՝ երաշխիքների վերաբերյալ տեղեկությունները, երբ անձնական տվյալները փոխանցվում են երրորդ երկիր կամ միջազգային կազմակերպություն	Հոդված 15(2)
5.	Հսկողի՝ մշակվող անձնական տվյալների կրկնօրինակը տրամադրելու պարտավորությունը	Հոդված 15(3), առաջին նախադասություն
6.	Հսկողի կողմից ողջամիտ վճարի գանձումը՝ հիմք ընդունելով տվյալների սուբյեկտի կողմից պահանջվող ցանկացած լրացուցիչ կրկնօրինակի համար կատարվող վարչական ծախսերը	Հոդված 15(3), երկրորդ նախադասություն
7.	Տեղեկությունների տրամադրումն էլեկտրոնային եղանակով	Հոդված 15(3), երրորդ նախադասություն
8.	Այլ անձանց իրավունքներն ու ազատությունները հաշվի առնելը	Հոդված 15(4)

Թեև 15(1) և (2) հոդվածի բոլոր տարրերը միասին սահմանում են հասանելիություն ունենալու իրավունքի բովանդակությունը, այնուամենայնիվ, 15(3) հոդվածը վերաբերում է հասանելիություն ապահովելու մեթոդներին՝ ի լրումն ՏՊԸԿ 12-րդ հոդվածով սահմանված ընդհանուր պահանջներին: 15(4) հոդվածով լրացվում են այն սահմաններն ու սահմանափակումները, որոնք ՏՊԸԿ 12(5) հոդվածով նախատեսվում է տվյալների բոլոր սուբյեկտների իրավունքների համար՝ հատուկ ուշադրություն դարձնելով հասանելիության համատեքստում այլ անձանց իրավունքներին ու ազատություններին:

2.2.1 Հասանելիություն ունենալու իրավունքի բովանդակության սահմանումը

17. 15(1) և (2) հոդվածը պարունակում է հետևյալ երեք հայեցակետերը. նախ՝ հաստատում, թե արդյոք դիմում ներկայացրած անձի անձնական տվյալները մշակվում են, թե ոչ, և եթե այո, ապա երկրորդը՝ այդ տվյալների հասանելիությունը և երրորդը՝ մշակման վերաբերյալ տեղեկությունները: Դրանք կարելի է դիտարկել որպես երեք տարբեր բաղադրիչներ, որոնք միասին կազմում են հասանելիություն ունենալու իրավունքը:

2.2.1.1 Հաստատում, թե «արդյոք» անձնական տվյալները մշակվում են, թե ոչ

18. Անձնական տվյալներին հասանելիություն ստանալու մասին դիմում ներկայացնելիս առաջին բանը, որ տվյալների սուբյեկտները պետք է իմանան, այն է, թե արդյոք հսկողը մշակում է իրենց վերաբերող տվյալները, թե ոչ: Հետևաբար, այս տեղեկատվությունը 15(1) հոդվածի համաձայն հասանելիություն ունենալու իրավունքի առաջին բաղադրիչն է: Եթե հսկողը չի մշակում հասանելիություն ստանալու դիմում ներկայացրած տվյալների սուբյեկտին վերաբերող անձնական տվյալները, ապա տրամադրվելիք տեղեկությունները սահմանափակվում են միայն հաստատելով, որ տվյալների սուբյեկտին վերաբերող ոչ մի անձնական տվյալ չի մշակվում: Եթե հսկողը մշակում է դիմում ներկայացրած անձին վերաբերող տվյալները, ապա նա պետք է տվյալ անձին հաստատի այդ փաստը: Այս հաստատումը կարող է ներկայացվել առանձին, կամ այն կարող է ներառվել որպես մշակվող անձնական տվյալների վերաբերյալ տեղեկությունների մաս (տե՛ս ստորև):

2.2.1.2 Մշակվող անձնական տվյալների հասանելիությունը

19. Անձնական տվյալներին հասանելիությունը 15(1) հոդվածով նախատեսված հասանելիություն ունենալու իրավունքի երկրորդ բաղադրիչն է, և այն կազմում է այս իրավունքի առանցքը: Այն վերաբերում է ՏՊԸԿ 4(1) հոդվածով սահմանված՝ անձնական տվյալների հասկացությանը: Բացի հիմնական անձնական տվյալներից՝ անունից ու հասցեից, այս սահմանման մեջ կարող են մտնել անսահմանափակ, տարատեսակ տվյալներ՝ պայմանով, որ դրանք ընկնում են ՏՊԸԿ նյութական շրջանակի ներքո, մասնավորապես՝ կապված դրանց մշակման եղանակի հետ (ՏՊԸԿ 2-րդ հոդված): Հետևաբար, անձնական տվյալներին հասանելիություն նշանակում է հասանելիություն հենց իրական անձնական տվյալներին, այլ ոչ միայն տվյալների ընդհանուր նկարագրությանը կամ պարզապես հղում՝ հսկողի կողմից մշակվող անձնական տվյալների կատեգորիաներին: Եթե ոչ մի սահման կամ սահմանափակում չի կիրառվում[12], ապա տվյալների սուբյեկտներն իրավունք ունեն հասանելիություն ստանալու իրենց վերաբերող մշակված բոլոր կամ տվյալների որոշ մասին՝ կախված դիմումի շրջանակից (տե՛ս 2.3.1 բաժինը): Տվյալներին հասանելիություն ապահովելու պարտավորությունը պայմանավորված չէ այդ տվյալների տեսակով կամ աղբյուրով: Այն ամբողջությամբ կիրառվում է նույնիսկ այն դեպքերում, երբ դիմում ներկայացրած անձն է հսկողին ի սկզբանե տրամադրած եղել տվյալները, քանի որ դրա նպատակը՝ տվյալների սուբյեկտին հսկողի կողմից այդ տվյալների իրական մշակման մասին տեղեկացնելն է: 15-րդ հոդվածով նախատեսված անձնական տվյալների շրջանակը մանրամասնորեն ներկայացված է 4.1 և 4.2 բաժիններում:

---

[12] Տե՛ս սույն Ուղեցույցի 6-րդ բաժինը:

2.2.1.3 Մշակման և տվյալների սուբյեկտի իրավունքների մասին տեղեկությունները

20. Հասանելիություն ունենալու իրավունքի երրորդ բաղադրիչը մշակման և տվյալների սուբյեկտների իրավունքների վերաբերյալ տեղեկություններն են, որոնք հսկողը պետք է տրամադրի՝ 15(1)(ա)-(ը) և 15(2) հոդվածների համաձայն: Այդ տեղեկությունները կարող են հիմնված լինել, օրինակ՝ հսկողի գաղտնիության մասին ծանուցումից[13] կամ ՏՊԸԿ 30-րդ հոդվածում նշված՝ հսկողի տվյալների մշակման գործողությունների հաշվառման մատյանից վերցված տեքստի վրա, ինչը սակայն պետք է թարմացվի և հարմարեցվի տվյալների սուբյեկտի դիմումին: Տեղեկությունների բովանդակության և հստակեցման աստիճանի վերաբերյալ առավել մանրամասն ներկայացված է 4.3 բաժնում:

2.2.2 Մեթոդների վերաբերյալ դրույթները

21. 15(3) հոդվածը հասանելիություն ստանալու մասին դիմումների համատեքստում որոշ հստակեցումներով լրացնում է ՏՊԸԿ 12-րդ հոդվածով սահմանված՝ հասանելիություն ստանալու մասին դիմումներին պատասխանելու մեթոդներին ներկայացվող պահանջները:

2.2.2.1 Կրկնօրինակի տրամադրումը

22. ՏՊԸԿ 15(3) հոդվածի առաջին նախադասության համաձայն՝ հսկողը տրամադրում է մշակմանն առնչվող անձնական տվյալների անվճար կրկնօրինակը: Հետևաբար, կրկնօրինակը վերաբերում է հասանելիություն ունենալու իրավունքի միայն երկրորդ բաղադրիչին («մշակված անձնական տվյալներին հասանելիություն», տե՛ս վերևում): Հսկողը պետք է ապահովի, որ առաջին կրկնօրինակը տրամադրվի անվճար, նույնիսկ եթե գտնի, որ վերարտադրման արժեքը բարձր է (օրինակ՝ հեռախոսազրույցի ձայնագրության կրկնօրինակի տրամադրման ծախսերը):

23. Կրկնօրինակը տրամադրելու պարտավորությունը չպետք է ընկալվի որպես տվյալների սուբյեկտի լրացուցիչ իրավունք, այլ պետք է ընկալվի որպես տվյալներին հասանելիություն ապահովելու մեթոդ: Այն ամրապնդում է տվյալների հասանելիություն ունենալու իրավունքը[14] և օգնում է մեկնաբանել այդ իրավունքը, քանի որ հստակ ցույց է տալիս, որ 15(1) հոդվածի համաձայն՝ տվյալներին հասանելիությունը ներառում է բոլոր տվյալների վերաբերյալ ամբողջական տեղեկություններ և չի կարող ընկալվել որպես միայն ամփոփ տվյալների տրամադրում: Միևնույն ժամանակ, կրկնօրինակը տրամադրելու պարտավորությունը նախատեսված չէ հասանելիություն ունենալու իրավունքի շրջանակն ընդլայնելու համար. այն վերաբերում է (միայն) մշակվող անձնական տվյալների կրկնօրինակին, և պարտադիր չէ, որ վերաբերի բնօրինակ փաստաթղթերի վերարտադրմանը (տե՛ս 5-րդ բաժինը, պարբերություն 152-րդ): Ընդհանուր առմամբ, կրկնօրինակը տրամադրելիս տվյալների սուբյեկտին չեն տրամադրվում լրացուցիչ տեղեկություններ. կրկնօրինակում պարունակվող տեղեկությունների շրջանակը, 15(1)հոդվածի համաձայն, տվյալներին հասանելիության շրջանակն է (վերը նշված հասանելիություն ունենալու իրավունքի երկրորդ բաղադրիչը, տե՛ս 19-րդ պարբերությունը), որը ներառում է այն բոլոր տեղեկությունները, որոնք անհրաժեշտ են տվյալների սուբյեկտին՝ հասկանալու մշակման գործընթացը և ստուգելու դրա

օրինականությունը[15]:

24. Վերը նշվածի լույսի ներքո, եթե 15(1) հոդվածի իմաստով տվյալներին հասանելիությունն ապահովվում է կրկնօրինակի տրամադրման միջոցով, ապա 15(3) հոդվածում նշված կրկնօրինակի տրամադրման պարտավորությունը կատարված է: Կրկնօրինակը տրամադրելու պարտավորությունը ծառայում է հասանելիություն ունենալու իրավունքի նպատակներին՝ թույլ տալով տվյալների սուբյեկտին տեղեկանալ մշակման մասին և ստուգել դրա օրինականությունը (63-րդ ներածական դրույթ): Այս նպատակներին հասնելու համար տվյալների սուբյեկտը շատ դեպքերում պետք է տեղեկությունները տեսնի ոչ միայն ժամանակավորապես: Հետևաբար, տվյալների սուբյեկտին անհրաժեշտ կլինի տեղեկություններին հասանելիություն ստանալ՝ անձնական տվյալների կրկնօրինակն ստանալու միջոցով:

25. Հաշվի առնելով վերը նշվածը՝ կրկնօրինակի գաղափարը պետք է մեկնաբանվի լայն իմաստով և ներառի անձնական տվյալներին հասանելիության տարբեր տեսակներ, եթե դրանք ամբողջական են (այսինքն՝ այն ներառում է բոլոր պահանջվող անձնական տվյալները), և եթե տվյալների սուբյեկտը կարող է դրանք պահպանել: Այսպիսով, կրկնօրինակ տրամադրելու պահանջը նշանակում է, որ դիմում ներկայացնող անձի վերաբերյալ անձնական տվյալների մասին տեղեկությունները տրամադրվում են տվյալների սուբյեկտին այնպես, որ տվյալների սուբյեկտին հնարավորություն է տալիս պահպանել ամբողջ տեղեկությունները և վերադառնալ դրան:

26. Չնայած կրկնօրինակի հասկացության այս լայն ըմբռնմանը, և հաշվի առնելով, որ այն հանդիսանում է հասանելիություն ապահովելու հիմնական մեթոդը՝ այնուամենայնիվ, մյուս մեթոդների կիրառումը որոշ հանգամանքներում կարող է նպատակահարմար լինել: Կրկնօրինակների և հասանելիություն ապահովելու մյուս մեթոդների վերաբերյալ հավելյալ պարզաբանումները ներկայացված են 5-րդ բաժնում, մասնավորապես՝ 5.2.2-5.2.5 ենթաբաժնում:

---

[13] Տե՛ս 29-րդ հոդվածով սահմանված աշխատանքային խմբի մասին տեղեկությունները, WP260 rev.01, 2018 թվականի ապրիլի 11, ՏՊԵԽ-ի կողմից հաստատված՝ 2016/679 կանոնակարգի համաձայն թափանցիկության վերաբերյալ ուղեցույց (այսուհետ՝ ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց):

[14] Կրկնօրինակը տրամադրելու պարտավորության մասին չի հիշատակվում Տվյալների պաշտպանության մասին 95/46/ԵՀ հրահանգում:

[15] Սույն պարբերության թեմային առնչվող հարցերը հանդիսանում են ԵՄԱԴ-ում ներկայումս քննվող գործի քննության առարկա (C- 487/21):

2.2.2.2 Լրացուցիչ կրկնօրինակներ տրամադրելը

27. 15(3) հոդվածի երկրորդ նախադասությունը վերաբերում է այն իրավիճակներին, երբ տվյալների սուբյեկտը խնդրում է հսկողին իրեն տրամադրել մեկից ավելի կրկնօրինակներ, օրինակ, եթե առաջին կրկնօրինակը կորել կամ վնասվել է, կամ տվյալների սուբյեկտը ցանկանում է կրկնօրինակը ներկայացնել մեկ այլ անձի, կամ վերահսկող մարմին: Հիմք ընդունելով այն հանգամանքը, որ տվյալների սուբյեկտի դիմումի համաձայն հսկողը պետք է տրամադրի լրացուցիչ կրկնօրինակներ՝ 15(3) հոդվածը սահմանում է, որ ցանկացած լրացուցիչ կրկնօրինակի համար հսկողը կարող է գանձել ողջամիտ վճար՝ հաշվի առնելով կատարվող վարչական ծախսերը (15(3) հոդվածի երկրորդ նախադասություն):

28. Եթե տվյալների սուբյեկտն առաջին դիմումն ուղարկելուց հետո խնդրում է իրեն տրամադրել լրացուցիչ կրկնօրինակ, ապա կարող են հարցեր առաջանալ, թե արդյոք դա պետք է դիտարկվի որպես նոր դիմում, թե տվյալների սուբյեկտը ցանկանում է ստանալ տվյալների լրացուցիչ կրկնօրինակը՝ 15(3) հոդվածի երկրորդ նախադասության իմաստով, որի դեպքում լրացուցիչ կրկնօրինակի համար կարող է գանձվել վճար: Այս հարցերի պատասխանը կախված է բացառապես դիմումի բովանդակությունից. դիմումը պետք է մեկնաբանվի որպես լրացուցիչ կրկնօրինակ ձեռք բերելու խնդրանք այնքանով, որքանով այն ժամանակի և ծավալի առումով վերաբերում է անձնական տվյալների նույն մշակմանը, ինչ նախկին դիմումը: Այնուամենայնիվ, եթե տվյալների սուբյեկտը նպատակ ունի տեղեկություններ ստանալու մեկ այլ ժամանակի պահին մշակված տվյալների կամ ի սկզբանե պահանջվող տվյալներից տարբերվող այլ տվյալների վերաբերյալ, ապա 15(3) հոդվածի համաձայն անվճար օրինակը ձեռք բերելու իրավունքը կիրառվում է ևս մեկ անգամ: Սա գործում է նաև այն դեպքերում, երբ տվյալների սուբյեկտը դրանից կարճ ժամանակ առաջ ներկայացրել է առաջին դիմումը: Տվյալների սուբյեկտը կարող է իրացնել հասանելիություն ունենալու իր իրավունքը՝ հետագա դիմումի միջոցով և ստանալ անվճար օրինակը, եթե դիմումը 12(5) հոդվածի համաձայն չի դիտարկվում որպես սահմանազանցող՝ 12(5)(ա) հոդվածին համապատասխան ողջամիտ վճար գանձելու հնարավորությամբ (կրկնվող դիմումների սահմանազանցող բնույթի մասին տե՛ս 6-րդ բաժինը):

> **Օրինակ 2.** Հաճախորդը հասանելիություն ստանալու մասին դիմում է ներկայացնում առևտրային ընկերություն: Ընկերության պատասխանից մեկ տարի անց նույն հաճախորդը 15-րդ հոդվածի համաձայն հասանելիություն ստանալու մասին դիմում է ներկայացնում նույն ընկերություն: Անկախ նրանից, թե նախորդ դիմումից հետո կողմերի միջև կնքվել են նոր բիզնես գործարքներ, կամ նրանց միջև հաստատվել են այլ շփումներ, այս երկրորդ դիմումը պետք է դիտարկվի որպես նոր դիմում: Նույնիսկ եթե ընկերության կողմից տվյալների մշակման մեջ որևէ փոփոխություն տեղի չի ունեցել, ինչը պարտադիր չէ, որ ակնհայտ լինի տվյալների սուբյեկտի համար, ապա տվյալների սուբյեկտն իրավունք ունի ստանալու տվյալների անվճար կրկնօրինակը:
>
> **Այլ տարբերակ 1.** Նույնիսկ եթե հաճախորդը վերը նշված դեպքերում նոր դիմում է ներկայացնում, օրինակ՝ առաջին դիմումից միայն մեկ շաբաթ անց, ապա դա կարող է համարվել որպես նոր դիմում՝ համաձայն 15(1) և (3) հոդվածի առաջին նախադասության, եթե դա չի մեկնաբանվում որպես առաջին դիմումի զուտ հիշեցում: Նոր դիմումի կարճ ժամանակահատվածի և դրա կոնկրետ հանգամանքների առնչությամբ քննության առարկան է 12(5) հոդվածի համաձայն դրա սահմանազանցումը (տե՛ս 6-րդ բաժինը):
>
> **Այլ տարբերակ 2.** Ի պատասխան նախորդ դիմումի՝ օրինակի ձևով արդեն իսկ տրամադրված տեղեկությունների «նոր օրինակը» ստանալու մասին դիմումը, ենթադրենք, եթե հաճախորդը կորցրել է նախկինում ստացած օրինակը, պետք է, անշուշտ, դիտարկվի որպես լրացուցիչ կրկնօրինակ ստանալու մասին դիմում, քանի որ այն մշակման ծավալով և ժամանակով վերաբերում է նախորդ դիմումին:

29. Եթե տվյալների սուբյեկտը կրկին ներկայացնում է հասանելիություն ստանալու մասին առաջին հարցումը՝ այն հիմքերով, որ ստացված պատասխանն ամբողջական չի եղել կամ

մերժման հիմքերը նշված չեն եղել, ապա այդ դիմումը չպետք է դիտարկվի որպես նոր դիմում, քանի որ այն ընդամենն առաջին չբավարարված դիմումի մասին հիշեցում է:

30. Լրացուցիչ կրկնօրինակ ստանալու մասին դիմումների դեպքում ծախսերի բաշխման առնչությամբ 15(3) հոդվածով սահմանվում է, որ հսկողը կարող է գանձել ողջամիտ վճար՝ հաշվի առնելով դիմումին ընթացք տալու պատճառով առաջացած վարչական ծախսերը: Սա նշանակում է, որ վարչական ծախսերը հանդիսանում են կարևոր չափանիշ՝ վճարի չափը սահմանելու համար: Միևնույն ժամանակ, վճարը պետք է լինի համապատասխան՝ հաշվի առնելով հասանելիություն ունենալու իրավունքի կարևորությունը՝ որպես տվյալների սուբյեկտի հիմնարար իրավունք: Հսկողը չպետք է տվյալների սուբյեկտի վրա դնի վերադիր ծախսերը կամ մյուս ընդհանուր ծախսերը, այլ պետք է շեշտը դնի լրացուցիչ կրկնօրինակի տրամադրման արդյունքում առաջացած հատուկ ծախսերի վրա: Այս գործընթացը կազմակերպելիս հսկողը պետք է արդյունավետորեն օգտագործի իր մարդկային և նյութական ռեսուրսները՝ կրկնօրինակի ծախսերը ցածր պահելու համար, այդ թվում, եթե հսկողը ներգրավում է արտաքին աջակցություն:

31. Եթե հսկողը որոշում է գանձել վճար, ապա նա պետք է նախապես նշի, որ գանձվելու է վճար, և պետք է հնարավորինս հստակ նշի այն ծախսերի չափը, որը նախատեսում է գանձել տվյալների սուբյեկտից, ինչը հնարավորություն է տալիս տվյալների սուբյեկտին որոշելու՝ պահպանել կամ չեղարկել դիմումը:

2.2.2.3 Տեղեկությունները լայնորեն կիրառվող էլեկտրոնային եղանակով հասանելի դարձնելը

32. Էլեկտրոնային միջոցներով ներկայացված դիմումի դեպքում տեղեկությունները տրամադրվում են էլեկտրոնային միջոցներով, եթե դա հնարավոր է, և եթե տվյալների սուբյեկտն այլ բան չի պահանջում (տե՛ս ՏՊԸԿ 12(3) հոդվածը): 15(3) հոդվածի երրորդ նախադասությունը լրացնում է այս պահանջը հասանելիություն ստանալու մասին դիմումների համատեքստում՝ նշելով, որ հսկողը, ավելին, պարտավոր է պատասխանը տրամադրել լայնորեն կիրառվող էլեկտրոնային եղանակով, եթե տվյալների սուբյեկտն այլ բան չի պահանջում: 15(3) հոդվածով նախապես ենթադրվում է, որ հսկողները, որոնք հնարավորություն ունեն ստանալու էլեկտրոնային դիմումներ, կարող են դրա պատասխանը տրամադրել լայնորեն կիրառվող էլեկտրոնային եղանակով (մանրամասների համար տե՛ս 5.2.5 բաժինը): Այս դրույթը վերաբերում է բոլոր այն տեղեկություններին, որոնք պետք է տրամադրվեն 15(1) և (2) հոդվածի համաձայն: Հետևաբար, եթե տվյալների սուբյեկտը հասանելիություն ստանալու մասին դիմումը ներկայացնում է էլեկտրոնային միջոցներով, ապա բոլոր տեղեկությունները պետք է տրամադրվեն լայնորեն կիրառվող էլեկտրոնային եղանակով: Ձևաչափի հետ կապված հարցերն առավել մանրամասն ուսումնասիրվում են 5-րդ բաժնում: Հսկողը պետք է մշտապես կիրառի անվտանգության համապատասխան միջոցներ, մասնավորապես, երբ առնչվում է հատուկ կատեգորիայի անձնական տվյալների հետ (տե՛ս ստորև, 2.3.4 բաժնում):

2.2.3 Հասանելիություն ունենալու իրավունքի հնարավոր սահմանափակումը

33. Ի վերջո, հասանելիություն ունենալու իրավունքի համատեքստում, 15(4) հոդվածով նախատեսվում է հատուկ սահմանափակում: Այն նշում է, որ անհրաժեշտ է հաշվի առնել այլ անձանց իրավունքների ու ազատությունների վրա հնարավոր բացասական ազդեցությունները: Այս սահմանափակման շրջանակի և հետևանքների, ինչպես նաև ՏՊԸԿ 12(5) հոդվածով կամ ՏՊԸԿ 23-րդ հոդվածի համաձայն սահմանված լրացուցիչ սահմանների և սահմանափակումների վերաբերյալ հարցերը ներկայացված են 6-րդ բաժնում:

2.3 Հասանելիություն ունենալու իրավունքի ընդհանուր սկզբունքները

34. Երբ տվյալների սուբյեկտները դիմում են ներկայացնում իրենց տվյալներին հասանելիություն ստանալու նպատակով, ըստ էության, ՏՊԸԿ 15-րդ հոդվածում նշված տեղեկությունները պետք է միշտ տրամադրվեն ամբողջությամբ: Համապատասխանաբար, երբ հսկողը մշակում է տվյալների սուբյեկտին վերաբերող տվյալները, նա տրամադրում է 15(1) հոդվածում նշված բոլոր տեղեկությունները և, հարկ եղած դեպքում, 15(2) հոդվածում նշված տեղեկությունները: Հսկողը պետք է ձեռնարկի համապատասխան միջոցներ՝ ապահովելու համար, որ տեղեկությունները լինեն ամբողջական, ճշգրիտ և թարմացված, ինչպես նաև հնարավորինս մոտ՝ դիմումն ստանալու պահին տվյալների մշակման վիճակին[16]: Եթե երկու կամ ավելի հսկողներ տվյալները մշակում են համատեղ, ապա համատեղ հսկողների՝ տվյալների սուբյեկտի իրավունքների իրացման, հատկապես հասանելիություն ստանալու մասին դիմումներին պատասխանելու հետ կապված համապատասխան պարտականությունների վերաբերյալ պայմանավորվածությունը չի ազդում տվյալների սուբյեկտների իրավունքների վրա այն հսկողի առնչությամբ, որին հասցեագրված է իրենց դիմումը:[17]

2.3.1 Տեղեկությունների ամբողջականությունը

35. Բացի ստորև նշված բացառություններից՝ տվյալների սուբյեկտներն իրավունք ունեն իրենց վերաբերող բոլոր տվյալների ամբողջական տրամադրման (շրջանակի վերաբերյալ մանրամասների համար տե՛ս 4.2 բաժինը): Եթե տվյալների սուբյեկտն այլ բան ուղղակիորեն չի պահանջում, ապա հասանելիություն ունենալու իրավունքի իրացման մասին դիմումն ընկալվում է ընդհանուր հատկանիշներով՝ ընդգրկվելով տվյալների սուբյեկտին վերաբերող բոլոր անձնական տվյալները[18]: Տեղեկությունների մի մասի հասանելիության սահմանափակումը կարող է դիտարկվել հետևյալ դեպքերում՝

ա) տվյալների սուբյեկտը բացահայտորեն դիմել է տվյալների կոնկրետ ենթախումբ ստանալու համար: Թերի տեղեկությունների տրամադրումից խուսափելու համար հսկողը կարող է դիտարկել տվյալների սուբյեկտի դիմումի այս սահմանափակումը միայն այն դեպքում, երբ վստահ լինի, որ այս մեկնաբանությունը համապատասխանում է տվյալների սուբյեկտի ցանկությանը (լրացուցիչ մանրամասների համար տե՛ս 3.1.1 բաժինը, 51-րդ պարբերությունը): Ըստ էության, տվյալների սուբյեկտը չպետք է նորից ներկայացնի բոլոր այն տվյալների փոխանցման մասին դիմում, որոնք ստանալու իրավունքը նա ունի.

բ) այն դեպքերում, երբ հսկողը մշակում է տվյալների սուբյեկտին վերաբերող մեծ քանակությամբ տվյալներ, նա կարող է կասկածներ ունենալ, թե արդյոք հասանելիություն ստանալու մասին դիմումը, որը ներկայացվել է շատ ընդհանուր հատկանիշներով, իսկապես ուղղված է մշակվող բոլոր տեսակի տվյալների կամ հսկողի գործունեության բոլոր ոլորտների վերաբերյալ մանրամասն տեղեկություններ ստանալուն: Դրանք կարող են առաջանալ հատկապես այն դեպքերում, երբ հնարավորություն չի եղել տվյալների սուբյեկտին տրամադրել գործիքներ՝ իր դիմումը հենց սկզբից հստակեցնելու համար, կամ երբ տվյալների սուբյեկտը չի օգտվել դրանցից: Այդ դեպքում հսկողը բախվում է խնդիրների, թե ինչպես տրամադրել ամբողջական պատասխան՝ միաժամանակ խուսափելով տվյալների սուբյեկտին ավելորդ տեղեկություններ տրամադրելուց, որը նրան չի հետաքրքրում, և նա չի կարող դրանք արդյունավետորեն օգտագործել: Կարող են լինել այս խնդիրը լուծելու եղանակներ՝ կախված հանգամանքներից և տեխնիկական

հնարավորություններից, օրինակ՝ տրամադրելով առցանց միջավայրում ինքնասպասարկման գործիքներ (տե՛ս բազմաշերտ մոտեցման վերաբերյալ 5-րդ բաժինը): Եթե այդ լուծումները կիրառելի չեն, ապա հսկողը, որը մշակում է տվյալների սուբյեկտին վերաբերող մեծ քանակությամբ տեղեկություններ, կարող է պահանջել տվյալների սուբյեկտից՝ նախքան տեղեկությունների տրամադրումը, հստակեցնել այն տեղեկությունները կամ մշակումը, որին վերաբերում է դիմումը (տե՛ս ՏՊԸԿ 63-րդ ներածական դրույթը): Դրա օրինակները կարող են լինել՝ մի քանի ոլորտներում գործունեություն իրականացնող ընկերությունը կամ տարբեր վարչական ստորաբաժանումներ ունեցող պետական մարմինը, եթե հսկողը պարզել է, որ տվյալների սուբյեկտին վերաբերող բազմաթիվ տվյալներ մշակվում են այդ մասնաճյուղերում: Բացի դրանից, մեծ քանակությամբ տվյալներ կարող են մշակվել այն հսկողների կողմից, որոնք երկար ժամանակահատվածի ընթացքում տվյալների սուբյեկտի հաճախակի գործունեության վերաբերյալ տվյալներ են հավաքագրում:

Օրինակ 3. Պետական մարմինը մի շարք տարբեր դեպարտամենտներում մշակում է տվյալների սուբյեկտի վերաբերյալ տվյալներ՝ ելնելով տարբեր իրավիճակներից: Ֆայլերի կառավարումը և ֆայլերի պահպանումը մասամբ իրականացվում են ոչ ավտոմատացված միջոցներով, և տվյալների մեծ մասը պահվում է միայն թղթապանակներում: Ինչ վերաբերում է դիմումի ընդհանուր ձևակերպմանը՝ պետական մարմինը կասկածներ ունի այն մասին, թե արդյոք տվյալների սուբյեկտը ծանոթ է դիմումի ծավալին, հատկապես մշակման համար պահանջվող տարատեսակ գործողություններին, տեղեկությունների այն ծավալին ու էջերի քանակին, որոնք տվյալների սուբյեկտը կստանա:

Օրինակ 4. Խոշոր ապահովագրական ընկերությունը գրությամբ ստանում է տվյալների ընդհանուր հասանելիություն ստանալու մասին դիմում մի անձից, որը երկար տարիներ եղել է իր հաճախորդը: Թեև տվյալները ջնջելու ժամկետները լիովին պահպանված են, այնուամենայնիվ, ընկերությունը փաստացի մշակում է հաճախորդին վերաբերող հսկայական քանակությամբ տվյալներ, քանի որ տվյալների մշակումը դեռևս անհրաժեշտ է հաճախորդի հետ պայմանագրային հարաբերություններից բխող պայմանագրային պարտավորությունների (այդ թվում՝ անժամկետ պարտավորությունների, հաճախորդի և երրորդ անձանց, … հետ վիճելի հարցերի վերաբերյալ հաղորդակցության) կամ իրավական պարտավորությունների կատարման համար (արխիվացված տվյալներ, որոնք պետք է պահվեն հարկային նպատակներով և այլն): Ապահովագրական ընկերությունը կարող է կասկածներ ունենալ, թե արդյոք դիմումը, որը ներկայացվել է շատ ընդհանուր հատկանիշներով, իսկապես վերաբերում է այդ բոլոր տեսակների տվյալներին: Սա կարող է հատկապես խնդրահարույց լինել, եթե ապահովագրական ընկերությունն ունի տվյալների սուբյեկտի միայն փոստային հասցեն և, ուստի, պետք է ցանկացած տեղեկություն ուղարկի թղթային տարբերակով: Այնուամենայնիվ, նույն կասկածները կարող են տեղին լինել նաև այն դեպքում, երբ տեղեկությունները տրամադրվում են այլ միջոցներով:

Եթե նման դեպքերում հսկողը որոշում է դիմել տվյալների սուբյեկտին խնդրանքով հստակեցնել դիմումը, որպեսզի կատարի հասանելիություն ունենալու իրավունքի իրացումը դյուրացնելու իր պարտավորությունը (ՏՊԸԿ 12(2) հոդված), ապա հսկողը միաժամանակ տրամադրում է իր մշակման գործողությունների վերաբերյալ արժանահավատ տեղեկություններ, որոնք կարող են վերաբերել տվյալների սուբյեկտին՝ տեղեկացնելով իր գործունեության համապատասխան ոլորտների, տվյալների բազաների և այլնի մասին:

[16] Համապատասխան միջոցների վերաբերյալ ուղղորդման համար տե՛ս 5-րդ բաժինը, պարբերություններ 123-129:

[17] ՏՊԸԿ-ում «հսկող» և «մշակող» հասկացությունների վերաբերյալ ՏՊԵԽ-ի 07/2020 ուղեցույց, պարբերություն 162գ: Մշակողները պետք է աջակցեն հսկողին, նույն տեղում, պարբերություն 129:

[18] Բազմաշերտ մոտեցման թեմայի վերաբերյալ մանրամասների համար տե՛ս ստորև ներկայացված 5.2.3 բաժինը:

Օրինակ 5. Երբ աշխատանքային հարաբերություններում աշխատողը ներկայացնում է հասանելիություն ստանալու մասին ընդհանուր ձևակերպված դիմում, դրանից *որպես այդպիսին* պարզ չէ, թե նա ցանկանում է ստանալ օգտագործողի՝ համակարգ, աշխատավայր մուտք գործելու, ճաշարանում հաշվարկների, աշխատավարձի վճարումների և այլնի հետ կապված բոլոր տվյալները, թե ոչ: Գործատուի կողմից դիմումը հստակեցնելու պահանջի արդյունքում, օրինակ, կարող է պարզվել, որ աշխատողը ցանկանում է հասկանալ կամ ստուգել, թե ում է փոխանցվել իր կատարողականի գնահատումը: Եթե գործատուն աշխատողից չպահանջի հստակեցնել դիմումը, ապա աշխատողը կստանա մեծ քանակությամբ տեղեկություններ, որոնցից շատերը նրան անհրաժեշտ չեն: Միևնույն ժամանակ, գործատուն պետք է մշակման տարբեր իրավիճակների վերաբերյալ տրամադրի տեղեկություններ, որոնք կարող են վերաբերել աշխատողին, որպեսզի հնարավորություն տա վերջինիս համապատասխան կերպով հստակեցնել դիմումը:

Կարևոր է ընդգծել, որ հստակեցնելու պահանջը միտված չէ սահմանափակելու հասանելիություն ստանալու մասին դիմումի պատասխանը և չի օգտագործվում՝ տվյալների սուբյեկտին վերաբերող տվյալների կամ մշակման վերաբերյալ որևէ տեղեկություն թաքցնելու համար: Եթե տվյալների սուբյեկտը, որից պահանջվել է հստակեցնել իր դիմումի շրջանակը, հաստատում է իրեն վերաբերող բոլոր անձնական տվյալները ձեռք բերելու մտադրությունը, ապա հսկողն անշուշտ պետք է դրանք ամբողջությամբ տրամադրի:

Ամեն դեպքում հսկողը պետք է միշտ կարողանա ապացուցել, որ դիմումին ընթացք տալու եղանակը միտված է առավելագույնս գործողության մեջ դնել հասանելիություն ունենալու իրավունքը, և որ դա համահունչ լինի տվյալների սուբյեկտների իրավունքների իրացումը դյուրացնելու իր պարտավորությանը (ՏՊԸԿ 12(2)-րդ հոդված): Այս սկզբունքների համաձայն՝ հսկողը կարող է մինչև տվյալների սուբյեկտի ցանկության համաձայն լրացուցիչ տվյալներ տրամադրելը սպասել տվյալների սուբյեկտի պատասխանին, եթե հսկողը տվյալների սուբյեկտին տրամադրել է իրեն վերաբերող տվյալների մշակման բոլոր գործողությունների, այդ թվում՝ հատկապես այն գործողությունների հստակ, ամփոփ նկարագիրը, որոնք տվյալների սուբյեկտը կարող էր չակնկալել, եթե հսկողը նաև ապահովել է այն բոլոր տվյալներին հասանելիությունը, որոնք տվյալների սուբյեկտը ցանկացել է ձեռք բերել, և եթե, ավելին, այդ տեղեկություններն ուղեկցվել են հստակ նշումով, թե ինչպես կարելի է ձեռք բերել մշակված տվյալների մնացած մասերին հասանելիություն.

գ) կիրառվում են հասանելիություն ունենալու իրավունքի բացառությունները կամ սահմանափակումները (տե՛ս ստորև ներկայացված 6-րդ բաժնում): Նման դեպքերում հսկողը պետք է ուշադիր ստուգի, թե բացառությունը տեղեկությունների որ մասերին է վերաբերում և տրամադրի բոլոր տեղեկությունները, որոնք ներառված չեն այդ բացառության շրջանակում: Օրինակ՝ բացառությունը չի կարող ազդել ինքնին անձնական տվյալները մշակելու փաստի հաստատման վրա (բաղադրիչ 1): Արդյունքում, անհրաժեշտ է տրամադրել բոլոր անձնական տվյալների և 15(1) և (2) հոդվածում նշված բոլոր տեղեկությունների վերաբերյալ տեղեկություններ, որոնց վրա չեն տարածվում բացառությունը կամ սահմանափակումը:

2.3.2 Տեղեկությունների ճշգրտությունը

36. Տվյալների սուբյեկտին տրամադրված անձնական տվյալների օրինակում ներառված տեղեկությունները պետք է պարունակեն տվյալների սուբյեկտի մասին պահվող փաստացի տեղեկությունները կամ անձնական տվյալները: Սա ներառում է տեղեկությունների տրամադրման պարտավորություն այն տվյալների մասին, որոնք ճշգրիտ չեն կամ այն տվյալների մասին, որոնց մշակումն օրինական կամ այլևս օրինական չէ: Տվյալների սուբյեկտը կարող է, օրինակ՝ օգտվել հասանելիություն ունենալու իրավունքից՝ տարբեր հսկողների միջև շրջանառվող ոչ ճշգրիտ տվյալների աղբյուրը պարզելու համար: Եթե հսկողն ուղղել է ոչ ճշգրիտ տվյալները՝ մինչև տվյալների սուբյեկտին այդ մասին հայտնելը, ապա տվյալների սուբյեկտը զրկված կլինի այդ հնարավորությունից: Նույնը վերաբերում է անօրինական ճանապարհով մշակմանը: Տվյալների սուբյեկտին վերաբերող տվյալների՝ անօրինական ճանապարհով մշակման մասին տեղեկանալու հնարավորությունը հասանելիություն ունենալու իրավունքի հիմնական նպատակներից մեկն է: Մշակման անփոփոխ վիճակի մասին տեղեկացնելու պարտավորությունը չի հակասում հսկողի՝ անօրինական ճանապարհով մշակումը դադարեցնելու կամ ոչ ճշգրիտ տվյալներն ուղղելու պարտավորությանը: Այն հարցերի պատասխանները, թե ինչ հերթականությամբ պետք է կատարվեն այդ պարտավորությունները, ներկայացված են հետևյալ բաժնում:

2.3.3 Գնահատման ելակետային ժամանակը

37. Մշակվող տվյալների գնահատումն առավելագույնս հստակ արտացոլում է այն իրավիճակը, երբ հսկողն ստանում է դիմումը, իսկ պատասխանը պետք է ներառի այդ պահին առկա բոլոր տվյալները: Սա նշանակում է, որ հսկողը պետք է փորձի պարզել տվյալների սուբյեկտին վերաբերող տվյալների մշակման բոլոր գործողությունները՝ առանց անհարկի ձգձգման: Հետևաբար, հսկողները պարտավոր չեն տրամադրել այն անձնական տվյալները, որոնք նախկինում նրանց կողմից մշակվել են, սակայն այլևս չեն գտնվում իրենց տիրապետման ներքո[19]: Օրինակ՝ հսկողը կարող է ջնջել անձնական տվյալները՝ իր տվյալների պահպանման քաղաքականության և (կամ) օրենսդրական դրույթներին համապատասխան և այդպիսով այլևս չի կարող տրամադրել պահանջվող անձնական տվյալները: Այս համատեքստում պետք է հիշել, որ տվյալների պահպանման ժամկետը պետք է սահմանվի ՏՊԸԿ 5(1)(ե) հոդվածի համաձայն, քանի որ տվյալների ցանկացած պահպանում պետք է օբյեկտիվորեն հիմնավորված լինի:

38. Միևնույն ժամանակ, հսկողը նախօրոք ձեռնարկում է անհրաժեշտ միջոցներ, որպեսզի դյուրացնի հասանելիություն ունենալու իրավունքի իրացումը և հնարավորինս շուտ և մինչև տվյալները ջնջելն ընթացք տա այդ դիմումներին (տե՛ս 12(3) հոդվածը): Հետևաբար, պահպանման կարճ ժամկետների դեպքում դիմումին պատասխանելու համար ձեռնարկված միջոցները պետք է հարմարեցվեն պահպանման համապատասխան ժամկետին՝ հասանելիություն ունենալու իրավունքի իրացումը դյուրացնելու և դիմումի ներկայացման պահին մշակվող տվյալներին հասանելիություն ապահովելու մշտական անհնարինությունից խուսափելու համար[20]: Որոշ դեպքերում, այնուամենայնիվ, անհնար է լինում պատասխանել դիմումին՝ մինչև տվյալները ջնջելու համար նախատեսված ժամկետը: Օրինակ, եթե դիմումին հնարավորինս արագ պատասխանելու ընթացքում հսկողն առբերում է անձնական տվյալները, որոնք պետք է ջնջվեին հաջորդ օրը, ապա

հսկողին կարող է լրացուցիչ ժամանակ անհրաժեշտ լինել՝ դիտարկելու համար, թե արդյոք անհրաժեշտ է փոփոխություններ կատարել այլ անձանց ազատությունը պաշտպանելու համար՝ մինչև անձնական տվյալների կրկնօրինակը դիմում ներկայացրած անձին տրամադրելը: Եթե տվյալներն առբերվել են նախատեսված պահպանման ժամկետում, ապա հսկողը կարող է շարունակել մշակել այդ տվյալները՝ դիմումին պատասխանելու իր պարտավորությունը կատարելու նպատակով: Նման դեպքերում մշակումը կարող է հիմնված լինել ՏՊԸԿ 6(1)(գ) հոդվածի վրա՝ 15-րդ հոդվածի հետ համակցությամբ, և դրա տևողությունը պետք է համապատասխանի ՏՊԸԿ 12(3) հոդվածի պահանջներին[21]: Այս իրավական հիմքի կիրառումը սահմանափակվում է կոնկրետ դիմումին պատասխանելու համար անհրաժեշտ տվյալների մշակմամբ և չպետք է օգտագործվի որպես պահպանման ժամկետների ընդհանուր երկարաձգման հիմնավորում:

39. Ավելին, հսկողը չպետք է դիտավորյալ խուսափի պահանջվող անձնական տվյալները տրամադրելու պարտավորությունից՝ ոչնչացնելով կամ փոփոխելով անձնական տվյալները՝ ի պատասխան հասանելիություն ստանալու մասին դիմումի (տե՛ս 2.3.2 բաժինը): Եթե հասանելիություն ստանալու մասին դիմումը մշակելու ընթացքում հսկողը հայտնաբերում է ոչ ճշգրիտ տվյալներ կամ դրանց անօրինական ճանապարհով մշակում, ապա նա պետք է գնահատի մշակման վիճակը և համապատասխանաբար տեղեկացնի տվյալների սուբյեկտին՝ մինչև իր մյուս պարտավորությունները կատարելը: Իր շահերից ելնելով՝ այս մասին հետագա հաղորդակցության անհրաժեշտությունից խուսափելու, ինչպես նաև թափանցիկության սկզբունքը պահպանելու համար, հսկողը պետք է ավելացնի հետագա ուղղումների կամ ոչնչացումների մասին տեղեկություններ:

Օրինակ 6. Հասանելիություն ստանալու մասին դիմումին պատասխանելիս հսկողը գիտակցում է, որ իր ընկերությունում թափուր աշխատատեղի համար տվյալների սուբյեկտի կողմից ներկայացված դիմումը պահվել է պահպանման ժամկետից ավելի երկար: Այս դեպքում հսկողը չի կարող նախ ջնջել, հետո պատասխանել տվյալների սուբյեկտին, որ (դիմումի վերաբերյալ) որևէ տվյալ չի մշակվում: Այն պետք է նախ տրամադրի հասանելիություն, որից հետո նոր ջնջի տվյալները: Ոչնչացնելու մասին հետագա դիմումը կանխելու համար առաջարկվում է ավելացնել ջնջելու փաստի և ժամանակի մասին տեղեկություններ:

---

[19] Այդ նպատակով տե՛ս սույն ուղեցույցի 4-րդ բաժնի, ինչպես նաև Եվրոպական միության արդարադատության դատարանի 2009 թվականի մայիսի 7-ի C-553/07 գործում ներկայացված լրացուցիչ պարզաբանումները, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer* գործն անցյալի վերաբերյալ ստացողների կամ ստացողների կատեգորիաների մասին տեղեկությունների հասանելիություն ունենալու իրավունքի մասին:

[20] Օրինակ՝ կարող է դիտարկվել ինքնասպասարկման գործիքի ներդրման հնարավորությունը, որը տվյալների սուբյեկտին հնարավորություն է տալիս հեշտությամբ հասանելիություն ստանալ պահանջվող անձնական տվյալներին և ծանուցման համակարգին, որն զգուշացնում է հսկողին այն դիմումի մասին, որը վերաբերում է պահպանման կարճ ժամկետներ ունեցող անձնական տվյալներին՝ արագ գործողությունների իրականացումը դյուրացնելու նպատակով:

[21] Սա չի հակասում ապացուցման նպատակներով տվյալների հետագա մշակմանը՝ կապված հասանելիություն ստանալու մասին դիմումը համապատասխան ժամանակահատվածում մշակելու հետ:

Թափանցիկության սկզբունքը պահպանելու համար հսկողները պետք է տվյալների սուբյեկտին տեղեկացնեն մշակման կոնկրետ ժամանակի մասին, որին վերաբերում է հսկողի պատասխանը: Որոշ դեպքերում, օրինակ՝ հաճախակի հաղորդակցման գործողությունների համատեքստում, ելակետային ժամանակի միջակայքում, երբ գնահատվում է մշակումը, և ստացվում է հսկողի պատասխանը, կարող են տեղի ունենալ տվյալների լրացուցիչ մշակում կամ փոփոխություններ: Եթե հսկողը տեղյակ է այդ փոփոխություններից, ապա առաջարկվում է ներառել տեղեկություններ՝ այդ փոփոխությունների, ինչպես նաև դիմումին պատասխանելու համար անհրաժեշտ լրացուցիչ մշակման մասին:

2.3.4 Տվյալների անվտանգության պահանջների կատարումը

40. Քանի որ անձնական տվյալների փոխանցումը տվյալների սուբյեկտին և նրա համար դրանք հասանելի դարձնելը հանդիսանում են մշակման գործողություն, հսկողը պարտավոր է մշտապես ձեռնարկել համապատասխան տեխնիկական և կազմակերպչական միջոցներ՝ մշակման ռիսկին համապատասխան անվտանգության մակարդակ ապահովելու համար (տե՛ս ՏՊԸԿ 5(1)(զ), 24-րդ և 32-րդ հոդվածները): Սա կիրառվում է անկախ տվյալներին հասանելիություն ապահովելու մեթոդից: Տվյալների սուբյեկտին տվյալների ոչ էլեկտրոնային եղանակով փոխանցման դեպքում, կախված մշակման ռիսկերից, հսկողը կարող է դիտարկել պատվիրված փոստի օգտագործման կամ, որպես այլընտրանք, առաջարկել, սակայն չպարտավորեցնել տվյալների սուբյեկտին գործն անմիջապես հսկողի հաստատություններից մեկից ստորագրության դիմաց վերցնելու տարբերակը: Եթե 12-րդ հոդվածի (1) և (3) մասերի համաձայն՝ տեղեկությունները տրամադրվում են էլեկտրոնային միջոցներով, ապա հսկողն ընտրում է էլեկտրոնային միջոցներ, որոնք համապատասխանում են տվյալների անվտանգությանը ներկայացվող պահանջներին: Ինչպես նաև տվյալների կրկնօրինակը լայնորեն կիրառվող էլեկտրոնային եղանակով տրամադրելու դեպքում (տե՛ս 15(3) հոդվածը), հսկողը հաշվի է առնում տվյալների անվտանգությանը ներկայացվող պահանջները՝ ընտրելով էլեկտրոնային ֆայլը տվյալների սուբյեկտին փոխանցելու միջոցները: Սա կարող է ներառել գաղտնագրման կիրառում, գաղտնաբառով պաշտպանություն և այլն: Գաղտնագրված տվյալներին հասանելիությունը դյուրացնելու համար հսկողը պետք է նաև ապահովի, որ համապատասխան տեղեկությունները հասանելի լինեն, որպեսզի տվյալների սուբյեկտը կարողանա ստանալ վերծանված տեղեկությունները: Եթե տվյալների անվտանգությանը ներկայացվող պահանջներով կսահմանվի էլեկտրոնային նամակների ծայրից ծայր ծածկագրում, սակայն հսկողը կկարողանա ուղարկել միայն սովորական էլեկտրոնային նամակ, ապա նա ստիպված կլինի կիրառել այլ միջոցներ, ինչպես օրինակ՝ տվյալների սուբյեկտին (պատվիրված) փոստով ուղարկելով USB կրիչներ:

3 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՍՏԱՆԱԼՈՒ ՄԱՍԻՆ ԴԻՄՈՒՄՆԵՐԻՆ ՎԵՐԱԲԵՐՈՂ ԸՆԴՀԱՆՈՒՐ ԴԻՏԱՐԿՈՒՄՆԵՐԸ

3.1 Ներածություն

41. Անձնական տվյալներին հասանելիություն ստանալու մասին դիմումներ ստանալիս

հսկողը պետք է յուրաքանչյուր դիմում գնահատի անհատական կարգով: Հսկողը, *ի թիվս այլնի*, հաշվի է առնում հաջորդ կետերում առավել մանրամասն ներկայացված հարցերը. արդյո՞ք դիմումը վերաբերում է դիմում ներկայացրած անձի հետ կապված անձնական տվյալներին, և ո՞վ է դիմում ներկայացրած անձը: Այս բաժինը նպատակ ունի պարզաբանելու, թե հասանելիություն ստանալու մասին դիմումի որ տարրերը հսկողը պետք է հաշվի առնի իր գնահատումն իրականացնելիս և քննարկել այդ գնահատման հնարավոր սցենարները, ինչպես նաև դրանց հետևանքները: Անձնական տվյալներին հասանելիություն ստանալու մասին դիմումը գնահատելիս հսկողը պետք է հաշվի առնի նաև, ՏՊԸԿ 12(2) հոդվածի համաձայն, տվյալների սուբյեկտի իրավունքների իրացումը դյուրացնելու պարտավորությունը՝ նկատի ունենալով անձնական տվյալների համապատասխան անվտանգության ապահովումը[22]:

42. Հետևաբար, հսկողները պետք է պրոակտիվ կերպով պատրաստ լինեն ընթացք տալ անձնական տվյալներին հասանելիություն ստանալու մասին դիմումներին: Սա նշանակում է, որ հսկողը պետք է պատրաստ լինի ստանալ դիմումը, պատշաճ կերպով գնահատել այն (այս գնահատումը ուղեցույցի սույն բաժնի առարկան է) և առանց անհարկի ձգձգումների պատշաճ պատասխան տրամադրել դիմում ներկայացրած անձին: Այն եղանակը, որով հսկողները պատրաստվելու են բավարարել հասանելիություն ստանալու մասին դիմումները, պետք է լինի համարժեք ու համաչափ և կախված լինի մշակման բնույթից, շրջանակից, համատեքստից և նպատակներից, ինչպես նաև ֆիզիկական անձանց իրավունքներին ու ազատություններին սպառնացող ռիսկերից՝ ՏՊԸԿ 24-րդ հոդվածին համապատասխան: Կախված կոնկրետ հանգամանքներից՝ հսկողներից կարող է պահանջվել, օրինակ, իրականացնել համապատասխան ընթացակարգ, որի իրականացումը պետք է երաշխավորի տվյալների անվտանգությունը՝ չխոչընդոտելով տվյալների սուբյեկտի իրավունքների իրացումը:

3.1.1 Դիմումի բովանդակության վերլուծությունը

43. Այս հարցը կարելի է առավել կոնկրետ գնահատել՝ տալով հետևյալ հարցերը.

[22] Ամբողջականության և գաղտնիության սկզբունքին համապատասխան (ՏՊԸԿ 5(1)(զ) հոդված)՝ հսկողն ապահովում է անձնական տվյալների համապատասխան անվտանգությունը՝ ձեռնարկելով ՏՊԸԿ 32-րդ հոդվածում նշված և ՏՊԸԿ 24-րդ հոդվածում ներկայացված համապատասխան տեխնիկական և կազմակերպչական միջոցներ: Հսկողները պետք է կարողանան ապացուցել, որ ապահովում են տվյալների պաշտպանության համապատասխան մակարդակ՝ հաշվետվողականության սկզբունքին համահունչ (տե՛ս նաև 29-րդ հոդվածով սահմանված աշխատանքային խմբի 2010 թվականի հուլիսի 13-ին ընդունված՝ 3/2010 կարծիքը հաշվետվողականության սկզբունքի վերաբերյալ, 00062/10/EN WP 173 և ՏՊԸԿ-ում «հսկող» և «մշակող» հասկացությունների վերաբերյալ ՏՊԵԽ-ի թիվ 07/2020 ուղեցույց):

ա) <u>Արդյո՞ք դիմումը վերաբերում է անձնական տվյալներին</u>

44. ՏՊԸԿ համաձայն՝ դիմումի շրջանակը վերաբերում է միայն անձնական տվյալներին[23]: Հետևաբար, այլ հարցերի վերաբերյալ տեղեկություններ, այդ թվում՝ հսկողի, իր բիզնես մոդելների կամ անձնական տվյալներին չվերաբերող մշակման իր գործողությունների վերաբերյալ ընդհանուր տեղեկություններ ստանալու համար ներկայացված ցանկացած դիմում չպետք է դիտարկվի որպես ՏՊԸԿ 15-րդ հոդվածի համաձայն ներկայացված դիմում: Բացի դրանից, անանուն տվյալների կամ դիմումը ներկայացրած անձին կամ վերջինիս անունից դիմում ներկայացրած լիազորված անձին չվերաբերող տվյալների վերաբերյալ տեղեկություններ ստանալու դիմումը չի գտնվում հասանելիություն ունենալու իրավունքի գործողության ոլորտում: Այս հարցն առավել մանրամասն կվերլուծվի 4-րդ բաժնում:

45. Ի տարբերություն անանուն տվյալների (որոնք չեն հանդիսանում անձնական տվյալներ), կեղծանունացված տվյալները, որոնք կարող են վերագրվել ֆիզիկական անձին լրացուցիչ տեղեկությունների օգտագործմամբ, հանդիսանում են անձնական տվյալներ[24]: Այսպիսով, կեղծանունացված տվյալները, որոնք կարող են փոխկապակցվել տվյալների սուբյեկտի հետ, օրինակ, երբ տվյալների սուբյեկտը տրամադրում է համապատասխան նույնականացուցիչը, որը թույլ է տալիս իր նույնականացումը, կամ երբ հսկողը կարողանում է իր սեփական միջոցներով տվյալները կապել դիմում ներկայացրած անձի հետ, պետք է դիտարկվեն դիմումի շրջանակներում[25]:

բ) <u>Արդյո՞ք դիմումը վերաբերում է դիմում ներկայացրած անձին (կամ այն անձին, որի անունից լիազորված անձը ներկայացնում է դիմումը)</u>

46. Որպես կանոն՝ դիմումը կարող է վերաբերել միայն դիմում ներկայացնող անձի տվյալներին: Այլ անձանց տվյալներին հասանելիություն կարող է պահանջվել միայն համապատասխան թույլտվության առկայության դեպքում[26]:

Օրինակ 7. Տվյալների X սուբյեկտն աշխատում է որպես դեպարտամենտի ղեկավար մի ընկերությունում, որն ընկերության ավտոպարկում իր ղեկավարների համար կայանատեղեր է տրամադրում: Թեև տվյալների X սուբյեկտն ունի մշտական կայանատեղի, սակայն, երբ տվյալների սուբյեկտը գալիս է աշխատանքի իր երկրորդ հերթափոխի համար, այդ տարածքը հաճախ արդեն զբաղեցված է լինում մեկ այլ ավտոմեքենայով: Քանի որ տվյալ իրավիճակը կրում է մշտական բնույթ, անօրինական կերպով իր կայանատեղին զբաղեցնող վարորդին հայտնաբերելու համար, տվյալների սուբյեկտը խնդրում է գրասենյակի ավտոկայանատեղի տարածքը տեսանկարահանող համակարգի օպերատորին հասանելիություն տրամադրել այդ վարորդի անձնական տվյալներին: Նման դեպքում տվյալների X սուբյեկտի դիմումը չի հանդիսանա իր անձնական տվյալներին հասանելիություն տրամադրելու վերաբերյալ դիմում, քանի որ այն չի վերաբերում դիմում ներկայացնող անձի տվյալներին, այլ մեկ այլ անձի տվյալներին, հետևաբար, այն չպետք է դիտարկվի որպես դիմում՝ համաձայն ՏՊԸԿ 15-րդ հոդվածի:

---

[23] Եթե դիմումը չի վերաբերում նաև տվյալների սուբյեկտի անձնական տվյալների հետ անքակտելիորեն կապված ոչ անձնական տվյալներին: Լրացուցիչ պարզաբանումների համար տե՛ս 100-րդ պարբերությունը:

[24] Տե՛ս ՏՊԸԿ 26-րդ ներածական դրույթը: «Անանուն տվյալներ» և «կեղծանունացված տվյալներ» հասկացությունների վերաբերյալ լրացուցիչ պարզաբանումներ կարելի է գտնել «Անձնական տվյալներ» հասկացության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի 4/2007 կարծիքում, էջեր 18-21:

[25] 29-րդ հոդվածով սահմանված աշխատանքային խումբ, WP242 rev.01, 2017 թվականի ապրիլի 5, ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ ուղեցույց (այսուհետ՝ ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց), էջ 9:

[26] Տե՛ս 3.4 բաժինը («Երրորդ անձանց/վստահված անձանց միջոցով ներկայացված դիմումները»):

գ) Արդյո՞ք ՏՊԸԿ-ի՝ որոշ կատեգորիաների տվյալների հասանելիությունը կարգավորող դրույթներից բացի այլ դրույթներ կիրառվում են

47. Տվյալների սուբյեկտները պարտավոր չեն իրենց դիմումի մեջ նշել իրավական հիմքը: Այնուամենայնիվ, եթե տվյալների սուբյեկտները պարզաբանում են, որ իրենց դիմումը հիմնված է որոշ կատեգորիաների տվյալների հասանելիության հատուկ հարցը կարգավորող ոլորտային օրենսդրության կամ ազգային օրենսդրության վրա, այլ ոչ թե ՏՊԿԸ-ի վրա, ապա այդ դիմումն ուսումնասիրվում է հսկողի կողմից՝ ոլորտային կամ ազգային այդ կանոնների համապատասխան, եթե դրանք կիրառելի են: Հաճախ, հիմք ընդունելով համապատասխան ազգային օրենսդրությունը, հսկողներից կարող է պահանջվել տրամադրել առանձին պատասխաններ, որոնցից յուրաքանչյուրը վերաբերում է տարբեր օրենսդրական ակտերով սահմանված հատուկ պահանջներին: Սա չպետք է շփոթել հասանելիություն ունենալու իրավունքի սահմանափակումներ սահմանող ազգային կամ ԵՄ օրենսդրության հետ, որոնք պետք է պահպանվեն հասանելիություն ստանալու մասին դիմումներին պատասխանելիս:

48. Եթե հսկողը կասկածներ ունի, թե որ իրավունքն է տվյալների սուբյեկտը ցանկանում իրացնել, ապա ցանկալի է դիմել դիմում ներկայացրած տվյալների սուբյեկտին խնդրանքով հաստակեցնել դիմումի առարկան: Տվյալների սուբյեկտի հետ այդ նամակագրությունը չի ազդում հսկողի՝ առանց անհարկի ձգձգումների գործելու պարտականության վրա[27]: Այնուամենայնիվ, կասկածների դեպքում, եթե հսկողը խնդրում է տվյալների սուբյեկտին տրամադրել լրացուցիչ պարզաբանումներ և պատասխան չի ստանում՝ նկատի ունենալով անձի հասանելիություն ունենալու իրավունքի իրացումը դյուրացնելու պարտավորությունը, ապա հսկողը պետք է մեկնաբանի առաջին դիմումի մեջ ներառված տեղեկությունները և գործի դրան համապատասխան: Հաշվետվողականության սկզբունքին համապատասխան՝ հսկողը կարող է որոշել համապատասխան ժամկետը, որի ընթացքում տվյալների սուբյեկտը կարող է տրամադրել լրացուցիչ պարզաբանումներ: Այդ ժամկետը սահմանելիս հսկողը պետք է բավարար ժամանակ թողնի դրա ավարտից հետո դիմումը բավարարելու համար, հետևաբար, հաշվի առնի, թե որքան ժամանակ է օբյեկտիվորեն անհրաժեշտ պահանջվող տվյալները՝ տվյալների սուբյեկտի կողմից հստակեցվելուց (կամ չհստակեցվելուց) հետո հավաքագրելու և տրամադրելու համար:

49. Եթե դիմումը ներկայացվում է ՏՊԸԿ շրջանակում, ապա այդ հատուկ օրենսդրության առկայությամբ ՏՊԸԿ-ով նախատեսված՝ հասանելիություն ունենալու իրավունքի ընդհանուր կիրառությունը չի չեղարկվում: Կարող են լինել ԵՄ կամ ազգային իրավունքով սահմանված սահմանափակումներ, երբ դա թույլատրվի ՏՊԸԿ 23-րդ հոդվածով (տե՛ս 6.4 բաժինը):

[27] Տե՛ս նաև 5.3 բաժնում ներկայացված՝ ժամկետների վերաբերյալ ուղեցույցը:

դ) <u>Արդյո՞ք դիմումը գտնվում է 15-րդ հոդվածի գործողության ոլորտում</u>

50. Հարկ է նշել, որ տվյալներին հասանելիություն պահանջող անձանց նկատմամբ ՏՊԸԿ-ով որևէ ձևական պահանջ չի ներկայացվում: Հասանելիություն ստանալու մասին դիմում ներկայացնելու համար բավարար է, որ դիմում ներկայացնող անձինք նշեն, որ ցանկանում են իմանալ, թե իրենց վերաբերող ինչ անձնական տվյալներ է հսկողը մշակում: Հետևաբար, հսկողը չի կարող հրաժարվել տվյալների տրամադրումից՝ հղում կատարելով դիմումի իրավական հիմքը չնշելու, հատկապես հասանելիություն ունենալու իրավունքին կամ ՏՊԸԿ-ին հատուկ հղում չկատարելու հանգամանքին:

Օրինակ՝ դիմում ներկայացնելու համար բավարար կլինի, որ դիմում ներկայացնող անձը նշի, որ.

- ցանկանում է հասանելիություն ստանալ իրեն վերաբերող անձնական տվյալներին.
- իրացնում է հասանելիություն ունենալու իր իրավունքը. կամ
- ցանկանում է իմանալ, թե հսկողն իրեն վերաբերող ինչ տեղեկություններ է մշակում:

Պետք է նկատի ունենալ, որ դիմողները կարող են ծանոթ չլինել ՏՊԸԿ նրբություններին, և որ պետք է համբերատար լինել այն անձանց հետ, որոնք իրացնում են իրենց հասանելիություն ունենալու իրավունքը, հատկապես, երբ այն իրացվում է անչափահասների կողմից: Ինչպես վերևը նշվեց, ցանկացած կասկածի դեպքում ցանկալի է, որ հսկողը խնդրի դիմում ներկայացնող տվյալների սուբյեկտին հստակեցնել դիմումի առարկան:

ե) <u>Արդյո՞ք տվյալների սուբյեկտները ցանկանում են հասանելիություն ունենալ իրենց վերաբերյալ մշակված բոլոր տեղեկություններին, թե դրանց մի մասին</u>

51. Բացի դրանից, հսկողը պետք է գնահատի, թե արդյոք դիմում ներկայացրած անձանց դիմումները վերաբերում են իրենց վերաբերյալ մշակված բոլոր տեղեկություններին, թե դրանց մի մասին: Տվյալների սուբյեկտների կողմից ներկայացված դիմումի շրջանակի՝ ՏՊԸԿ 15-րդ հոդվածի հատուկ դրույթով ցանկացած սահմանափակում պետք է լինի պարզ և ոչ երկիմաստ: Օրինակ, եթե տվյալների սուբյեկտները պահանջում են «իրենց առնչությամբ մշակված տվյալների վերաբերյալ բառացի տեղեկություններ», ապա հսկողը պետք է ենթադրի, որ տվյալների սուբյեկտները մտադիր են իրացնել իրենց լիարժեք իրավունքը՝ ՏՊԸԿ 15(1)-(2) հոդվածի համաձայն: Այդ դիմումը չպետք է մեկնաբանվի այն իմաստով, որ տվյալների սուբյեկտները ցանկանում են ստանալ միայն այն կատեգորիաների անձնական տվյալները, որոնք մշակվում են և հրաժարվել 15(1)(ա)-(ը) հոդվածներում նշված տեղեկություններն ստանալու իրավունքից: Իրավիճակն այլ կլինի, օրինակ, երբ տվյալների սուբյեկտներն իրենց կողմից մատնանշված տվյալների առնչությամբ ցանկանան հասանելիություն ունենալ անձնական տվյալների աղբյուրին կամ ծագմանը կամ պահպանման սահմանված ժամկետին: Նման դեպքում հսկողը կարող է տրամադրել միայն պահանջվող կոնկրետ տեղեկությունները:

3.1.2 Դիմումի ձևը

52. Ինչպես վերը նշվեց, անձնական տվյալներին հասանելիություն ստանալու մասին

դիմումի ձևի առնչությամբ ՏՊԸԿ-ն տվյալների սուբյեկտների համար որևէ պահանջ չի սահմանում: Ուստի, ՏՊԸԿ-ով սկզբունքորեն սահմանված չեն պահանջներ, որոնք տվյալների սուբյեկտները պետք է կատարեն այնպիսի հաղորդակցման ուղի ընտրելիս, որով նրանք կապ են հաստատում հսկողի հետ:

53. ՏՊԵԽ-ը խրախուսում է հսկողներին տրամադրել ամենանպատակահարմար և հեշտ կիրառելի հաղորդակցման ուղիներ, ՏՊԸԿ 12(2) և 25-րդ հոդվածներին համահունչ՝ տվյալների սուբյեկտին արդյունավետ դիմում ներկայացնելու հնարավորություն ընձեռելու համար: Այնուամենայնիվ, եթե տվյալների սուբյեկտը դիմումը ներկայացնում է՝ օգտագործելով հսկողի կողմից տրամադրված հաղորդակցման ուղին[28], որը տարբերվում է որպես նախընտրելի տարբերակ ներկայացված տարբերակից, ապա այդ դիմումը, ընդհանուր առմամբ, համարվում է արդյունավետ, և հսկողը պետք է համապատասխանաբար ընթացք տա այդ դիմումին (տե՛ս ստորև բերված օրինակները): Հսկողները պետք է ձեռնարկեն բոլոր ողջամիտ ջանքերը՝ համոզվելու համար, որ տվյալների սուբյեկտի իրավունքների իրացումը դյուրացված է (օրինակ, եթե տվյալների սուբյեկտը հասանելիություն ստանալու մասին դիմումն ուղարկում է արձակուրդում գտնվող աշխատողին, ապա ավտոմատ հաղորդագրությունը, որով տվյալների սուբյեկտը կտեղեկանա այդ դիմումը ներկայացնելու համար այլընտրանքային հաղորդակցման ուղիների մասին, կարող է լինել ողջամիտ քայլ):

54. Հարկ է նշել, որ հսկողը պարտավոր չէ ընթացք տալ վերջինիս կողմից անմիջապես չտրամադրված՝ պատահական կամ սխալ էլեկտրոնային (կամ փոստային) հասցեով կամ տվյալների սուբյեկտի իրավունքների իրացմանն առնչվող դիմումներ ստանալու համար հստակ չնախատեսված հաղորդակցման որևէ այլ ուղիներով ուղարկված դիմումին, եթե հսկողը տրամադրել է համապատասխան հաղորդակցման ուղի, որը տվյալների սուբյեկտը կարող է օգտագործել:

55. Հսկողը պարտավոր չէ նաև ընթացք տալ իր այն աշխատողի էլեկտրոնային հասցեին ուղարկված դիմումին, որը կարող է ներգրավված չլինել տվյալների սուբյեկտների իրավունքների իրացմանն առնչվող դիմումների մշակման գործում (օրինակ՝ վարորդներ, մաքրման ծառայության աշխատողներ և այլն): Այդ դիմումներն արդյունավետ չեն համարվում, եթե հսկողը տվյալների սուբյեկտին հստակ տրամադրել է հաղորդակցման համապատասխան ուղիներ: Այնուամենայնիվ, եթե տվյալների սուբյեկտը դիմում է ուղարկում հսկողի այն աշխատողին, որը նշանակված է եղել որպես մշտական կոնտակտային անձ (օրինակ՝ բանկում հաճախորդների հարցերով կառավարիչը կամ բջջային կապի օպերատորի մշտական խորհրդատուն), ապա այդ շփումը չպետք է համարվի պատահական, և հսկողը պետք է գործադրի բոլոր ողջամիտ ջանքերը՝ այդ դիմումին ընթացք տալու համար, որպեսզի այն հնարավոր լինի վերահասցեագրել կապի ապահովման կենտրոն և պատասխան տրամադրել ՏՊԸԿ-ով նախատեսված ժամկետներում:

[28] Սա կարող է ներառել, օրինակ՝ հսկողի՝ իր հաղորդակցություններում տրամադրված հաղորդակցման տվյալները՝ ուղղված անմիջականորեն տվյալների սուբյեկտներին կամ հսկողի կողմից հրապարակայնորեն, ինչպես օրինակ՝ հսկողի գաղտնիության քաղաքականությամբ կամ դրա՝ այլ պարտադիր իրավական ծանուցումներով (օրինակ՝ կայքում սեփականատիրոջ կամ ընկերության կոնտակտային տվյալներ) տրամադրված կոնտակտային տվյալները:

56. Այնուամենայնիվ, որպես լավագույն գործելակերպ՝ ՏՊԵԽ-ն առաջարկում է, որ հսկողները ներդնեն համապատասխան մեխանիզմներ՝ տվյալների սուբյեկտների իրավունքների իրացումը դյուրացնելու համար, այդ թվում՝ ներդնեն ինքնապատասխանիչ համակարգեր, որոնք կտեղեկացնեն աշխատողի՝ աշխատավայրում չլինելու և նրան փոխարինող համապատասխան աշխատողի մասին և, հնարավորության դեպքում, ներդնեն մեխանիզմներ՝ բարելավելու համար աշխատողների միջև ներքին հաղորդակցությունն այն աշխատողների կողմից ստացված դիմումների առնչությամբ, որոնք կարող են իրավասու չլինել այդ դիմումներին ընթացք տալու համար:

Օրինակ 8. X հսկողն ինչպես իր կայքում, այնպես էլ գաղտնիության մասին ծանուցման մեջ տրամադրում է էլեկտրոնային փոստի երկու հասցե՝

- հսկողի ընդհանուր էլեկտրոնային. փոստի հասցեն՝ CONTACT@X.COM և հսկողի տվյալների պաշտպանության հարցերով կապի ապահովման կենտրոնի էլեկտրոնային. փոստի հասցեն՝ QUERIES@X.COM: Բացի դրանից, X հսկողն իր կայքում նշում է, որ անձնական տվյալների մշակման առնչությամբ որևէ հարցում կամ դիմում ներկայացնելու համար անձինք պետք է կապ հաստատեն տվյալների պաշտպանության հարցերով կապի ապահովման կենտրոն՝ տրամադրված էլեկտրոնային. փոստի հասցեի միջոցով: Այնուամենայնիվ, տվյալների սուբյեկտը դիմումն ուղարկում է հսկողի ընդհանուր էլեկտրոնային. փոստի հասցեին՝ CONTACT@X.COM:

Նման դեպքում հսկողը պետք է գործադրի բոլոր ողջամիտ ջանքերը, որպեսզի իր ծառայությունները տեղյակ լինեն ընդհանուր է էլեկտրոնային. փոստի հասցեով ներկայացված դիմումից՝ այն տվյալների պաշտպանության հարցերով կապի ապահովման կենտրոն վերահասցեագրելու և ՏՊԸԿ-ով նախատեսված ժամկետներում պատասխան տրամադրելու նպատակով: Ավելին, հսկողն իրավունք չունի երկարաձգելու դիմումին պատասխանելու ժամկետը զուտ այն պատճառով, որ տվյալների սուբյեկտը դիմում է ուղարկել հսկողի ընդհանուր է էլեկտրոնային. փոստի հասցեին, այլ ոչ թե դրա՝ տվյալների պաշտպանության հարցերով կապի ապահովման կենտրոնի էլեկտրոնային հասցեին:

Օրինակ 9. Y հսկողը ղեկավարում է ֆիթնես ակումբների ցանց: Y հսկողն իր կայքում և ֆիթնես ակումբի հաճախորդների գաղտնիության մասին ծանուցման մեջ նշում է, որ անձնական տվյալների մշակման հետ կապված ցանկացած հարցում կամ դիմում ներկայացնելու համար անձինք պետք է կապ հաստատեն հսկողի հետ հետևյալ էլեկտրոնային փոստի միջոցով՝ QUERIES@Y.COM: Այնուամենայնիվ, տվյալների սուբյեկտը դիմումն ուղարկում է հանդերձարանում գտած էլեկտրոնային փոստի հասցեին, որտեղ փակցված ծանուցմամբ նշվում է հետևյալը՝ «Եթե դուք գոհ չեք հանդերձարանի մաքրությունից, ապա խնդրում ենք կապ հաստատել CLEANERS@Y.COM հասցեով», որը Y ընկերության մաքրման ծառայության էլեկտրոնային փոստի հասցեն է: Մաքրման ծառայությունն ակնհայտորեն ներգրավված չէ ֆիթնես ակումբի տվյալների սուբյեկտների՝ հաճախորդների իրավունքների իրացման հետ կապված հարցերին ընթացք տալու գործընթացին: Թեև էլեկտրոնային փոստի հասցեն հասանելի էր ֆիթնես ակումբի տարածքում, այնուամենայնիվ, տվյալների սուբյեկտը ողջամտորեն չէր կարող ակնկալել, որ սա համապատասխան կոնտակտային հասցե է այդ դիմումների համար, քանի որ կայքով և գաղտնիության մասին ծանուցմամբ հստակ նշված է այն հաղորդակցման ուղու մասին, որը պետք է օգտագործվի տվյալների սուբյեկտների իրավունքների իրացման համար:

57. Հսկողի կողմից դիմումն ստանալու ամսաթիվը, որպես կանոն, համարվում է այն մեկամսյա ժամկետի սկիզբը, որի ընթացքում հսկողը պետք է տեղեկություններ տրամադրի դիմումի վերաբերյալ ձեռնարկված գործողությունների մասին՝ ՏՊԸԿ 12(3) հոդվածին համապատասխան (ժամկետների առնչությամբ լրացուցիչ ուղղորդումը ներկայացված է 5.3 բաժնում): ՏՊԵԽ-ը լավագույն գործելակերպ է համարում հսկողի կողմից դիմումների ստացումը գրավոր կերպով հաստատելու գործելակերպը, օրինակ՝ էլեկտրոնային նամակներ (կամ հնարավորության դեպքում փոստով տեղեկություններ) ուղարկելով դիմում ներկայացրած անձանց՝ հաստատելով, որ իրենց դիմումներն ստացվել են, և որ մեկամսյա ժամկետը գործում է X օրից մինչև Y օր:

3.2 Նույնականացումը և իսկորոշումը

58. Մշակման անվտանգությունն ապահովելու և անձնական տվյալների չարտոնված հրապարակման ռիսկը նվազագույնի հասցնելու համար հսկողը պետք է կարողանա պարզել, թե որ տվյալներն են վերաբերում տվյալների սուբյեկտին (նույնականացում) և

հաստատել այդ անձի ինքնությունը (իսկորոշում):

59. Հարկ է հիշել, որ այն իրավիճակներում, երբ անձնական տվյալների մշակման նպատակը չի պահանջում կամ այլևս չի պահանջում տվյալների սուբյեկտի նույնականացում, հսկողը կարող է չնույնականացնել՝ զուտ միայն տվյալների սուբյեկտների իրավունքները կատարելու համար՝ նաև տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքի լույսի ներքո: Այս իրավիճակները կարգավորվում են ՏՊԸԿ 11(1) հոդվածով:

60. ՏՊԸԿ 12(2) հոդվածով սահմանվում է, որ հսկողը չպետք է հրաժարվի տվյալների սուբյեկտի դիմումին ընթացք տալուց՝ վերջինիս իրավունքներն իրացնելու նպատակով, բացառությամբ այն դեպքերի, երբ հսկողը մշակում է անձնական տվյալներն այնպիսի նպատակով, որը չի պահանջում տվյալների սուբյեկտի նույնականացում, և ապացուցվում է, որ տվյալների սուբյեկտին նույնականացնելու իրավասություն չկա: Այդուհանդերձ, նման հանգամանքներում տվյալների սուբյեկտը կարող է որոշել լրացուցիչ տեղեկություններ տրամադրել, որոնք հնարավոր կդարձնեն այդ նույնականացումը (ՏՊԸԿ 11(2) հոդված)[29]:

61. Լոկ տվյալների սուբյեկտի դիմումը բավարարելու նպատակով հսկողը պարտավոր չէ տվյալների սուբյեկտին նույնականացնելու համար ձեռք բերել այդ լրացուցիչ տեղեկությունները՝ նաև տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքի լույսի ներքո: Այնուամենայնիվ, այն չպետք է հրաժարվի տվյալների սուբյեկտի կողմից տրամադրված լրացուցիչ տեղեկությունները վերցնելուց՝ նրա իրավունքների իրացմանն աջակցելու համար (ՏՊԸԿ 57-րդ ներածական դրույթ):

Օրինակ 10. X-ը շենքի տեսահսկման հետ կապված տվյալների հսկողն է: Համաձայն ՏՊԸԿ 11(1) հոդվածի՝ հսկողը պարտավոր չէ նույնականացնել բոլոր այն անձանց, որոնք մոնիթորինգի իրականացման ժամանակ ֆիքսվել են անվտանգության տեսախցիկով (նպատակ, որը չի պահանջում նույնականացում): Հսկողն ստանում է անձնական տվյալներին հասանելիություն ստանալու մասին դիմում այն անձից, որը պնդում է, որ ֆիքսվել է հսկողի տեսահսկման համակարգի կողմից: Հսկողի գործողությունները կախված կլինեն տրամադրված լրացուցիչ տեղեկություններից: Եթե դիմում ներկայացրած անձը նշում է կոնկրետ օր և ժամը, երբ տեսախցիկները կարող էին ֆիքսած լինել տվյալ իրադարձությունը, հավանական է, որ հսկողը կարողանա տրամադրել այդ տվյալներ (ՏՊԸԿ 11(2) հոդված): Այնուամենայնիվ, եթե հսկողը չի կարողանում նույնականացնել տվյալների սուբյեկտին (օրինակ, եթե հսկողը չի կարողանում համոզվել, որ դիմում ներկայացրած անձն իրականում տվյալների սուբյեկտն է, կամ եթե դիմումը վերաբերում է, օրինակ՝ նախկինում կատարված ձայնագրություններին, և նա ի վիճակի չէ մշակել այդքան մեծ քանակությամբ տվյալներ), ապա հսկողը կարող է հրաժարվել որևէ գործողություն ձեռնարկելուց, եթե ապացուցի, որ ի վիճակի չէ նույնականացնել տվյալների սուբյեկտին (ՏՊԸԿ 12(2) հոդված):

Օրինակ 11. C հսկողը մշակում է անձնական տվյալներ՝ իր կայքի օգտատերերին վարքագծային գովազդմանու հարցը լուծելու նպատակով: Վարքագծային գովազդի համար հավաքագրված անձնական տվյալները սովորաբար հավաքագրվում են թխուկների միջոցով և կապված են կեղծանունացված պատահական նույնականացուցիչների հետ: Տվյալների սուբյեկտ՝ պարոն X-ը C-ի հետ հասանելիություն ունենալու իրավունքն իրացնում է C-ի կայքի միջոցով: C-ն ի վիճակի է ճշգրիտ կերպով նույնականացնել պարոն X-ին՝ տվյալների սուբյեկտի վարքագծային գովազդը ցույց տալու համար՝ պարոն X-ի տերմինալային սարքավորումը կապելով իր գովազդային պրոֆիլին՝ տերմինալ մտցված թխուկների միջոցով: Այնուհետև C-ն պետք է նաև կարողանա ճշգրիտ կերպով նույնականացնել պարոն X-ին, որպեսզի նրան տրամադրի իր անձնական տվյալներին հասանելիություն, քանի որ կարելի է կապ գտնել մշակված տվյալների և տվյալների սուբյեկտի միջև: Հետևաբար, և հաշվի առնելով ՏՊԸԿ սկզբունքները, վերը նշված օրինակը չի գտնվում ՏՊԸԿ 11-րդ հոդվածի գործողության ոլորտում: Ավելի ճիշտ, վերը նշված օրինակում, C-ի նպատակները պահանջում են տվյալների սուբյեկտների նույնականացում, իսկ ՏՊԸԿ 11-րդ հոդվածը հասցեագրում է մշակման այն իրավիճակը, որը չի պահանջում նույնականացում, որտեղ հսկողը ՏՊԸԿ 11(1) հոդվածի իմաստով պարտավոր չէ մշակել լրացուցիչ տվյալներ՝ միայն ՏՊԸԿ-ն կատարելու նպատակով: Հետևաբար, որոշ դեպքերում կարիք չկա պահանջել լրացուցիչ տվյալներ՝ տվյալների սուբյեկտի իրավունքներն իրացնելու համար:

Այնուամենայնիվ, եթե պարոն X-ը փորձի իրացնել իր հասանելիություն ունենալու իրավունքն էլեկտրոնային նամակով կամ սովորական փոստով, ապա այս դեպքում C-ն այլ ելք չի ունենա, քան դիմել պարոն X-ին խնդրանքով տրամադրել «լրացուցիչ տեղեկություններ» (ՏՊԸԿ 12(6) հոդված), որպեսզի կարողանա նույնականացնել պարոն X-ի հետ կապված գովազդային պրոֆիլը: Այս դեպքում լրացուցիչ տեղեկությունները կլինեն պարոն X-ի տերմինալային սարքավորման մեջ պահվող թխուկների նույնականացուցիչը:

---

[29] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 13:

62. Եթե ապացուցվում է, որ հնարավոր չէ նույնականացնել տվյալների սուբյեկտին (ՏՊԸԿ 11-րդ հոդված), ապա հսկողը պետք է հնարավորության դեպքում դրա մասին տեղեկացնի տվյալների սուբյեկտին, քանի որ հսկողը պետք է առանց անհարկի ձգձգումների պատասխանի տվյալների սուբյեկտի դիմումներին և հիմնավորումներ ներկայացնի, եթե մտադիր չէ բավարարել այդ դիմումները: Այս տեղեկությունները պետք է տրամադրվեն միայն «հնարավորության դեպքում», քանի որ հսկողը կարող է իրավասու չլինել տեղեկացնելու տվյալների սուբյեկտներին, եթե նրանց նույնականացումն անհնար է:

63. Թե' նույնականացում չպահանջող, թե' պահանջող դեպքերում եթե հսկողը հիմնավոր կասկածներ ունի դիմում ներկայացնող ֆիզիկական անձի ինքնության առնչությամբ, ապա հսկողը կարող է պահանջել լրացուցիչ տեղեկություններ, որոնք անհրաժեշտ են տվյալների սուբյեկտի ինքնությունը հաստատելու համար (ՏՊԸԿ 12(6) հոդված):

64. ՏՊԸԿ-ով որևէ պահանջ չի սահմանվում տվյալների սուբյեկտի ինքնությունն իսկորոշելու համար: Այնուամենայնիվ, ՏՊԸԿ 11-րդ և 12-րդ հոդվածներով նշվում են տվյալների սուբյեկտի բոլոր իրավունքների, այդ թվում՝ անձնական տվյալների հասանելիություն ունենալու իրավունքի իրացման պայմանները:

65. Հարկ է հիշել, որ, որպես կանոն, հսկողը չի կարող պահանջել ավելի շատ անձնական տվյալներ, քան անհրաժեշտ է այդ իսկորոշման համար, և որ այդ տեղեկությունները պետք է օգտագործվեն միմիայն տվյալների սուբյեկտների դիմումը բավարարելու համար:

66. Հաճախ տվյալների սուբյեկտների և հսկողների միջև արդեն գոյություն ունեն իսկորոշման ընթացակարգեր: Հսկողները կարող են կիրառել իսկորոշման այդ ընթացակարգերը՝ հաստատելու համար տվյալների այն սուբյեկտների ինքնությունը, որոնք պահանջում են իրենց անձնական տվյալները կամ իրացնում են ՏՊԸԿ-ով շնորհված իրավունքները[30]: Հակառակ դեպքում հսկողները պետք է այդ նպատակով ներդնեն համապատասխան իսկորոշման ընթացակարգը[31]:

67. Այն դեպքերում, երբ հսկողը պահանջում է կամ տվյալների սուբյեկտի կողմից ստանում է լրացուցիչ տեղեկություններ, որոնք անհրաժեշտ են տվյալների սուբյեկտի ինքնությունը հաստատելու համար, հսկողը պետք է ամեն անգամ գնահատի, թե որ տեղեկություններն իրեն հնարավորություն կտան հաստատելու տվյալների սուբյեկտի ինքնությունը և, հնարավորության դեպքում լրացուցիչ հարցեր տա դիմում ներկայացնող անձին կամ տվյալների սուբյեկտից պահանջի որոշ լրացուցիչ նույնականացման տարրեր ներկայացնել, եթե դա համաչափ է (տե՛ս 3.3 բաժինը):

[30] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 14:

[31] Իսկորոշման վերաբերյալ լրացուցիչ ուղղորդման համար տե՛ս 3.3 բաժինը:

68. Որպեսզի տվյալների սուբյեկտը կարողանա տրամադրել իր տվյալները նույնականացնելու համար անհրաժեշտ լրացուցիչ տեղեկություններ, հսկողը պետք է տվյալների սուբյեկտին տեղեկացնի նույնականացումը հնարավոր դարձնելու համար անհրաժեշտ լրացուցիչ տեղեկությունների բնույթի մասին: Այդ լրացուցիչ տեղեկությունները չպետք է լինեն ավելին, քան տվյալների սուբյեկտի իսկորոշման համար ի սկզբանե անհրաժեշտ տեղեկությունները: Ընդհանուր առմամբ, այն փաստը, որ հսկողը կարող է լրացուցիչ տեղեկություններ պահանջել տվյալների սուբյեկտի ինքնությունը գնահատելու համար, չի կարող հանգեցնել սահմանազանցող պահանջների և այնպիսի անձնական տվյալների հավաքագրման, որոնք վերաբերելի կամ անհրաժեշտ չեն անձի և պահանջվող անձնական տվյալների միջև կապն ամրապնդելու համար[32]:

69. Հետևաբար, երբ առցանց հավաքագրված տեղեկությունները կապված են կեղծանունացված կամ այլ եզակի նույնականացուցիչների հետ, հսկողը կարող է կիրառել համապատասխան ընթացակարգեր, որոնք հնարավորություն են տալիս դիմում ներկայացնող անձին ներկայացնել տվյալներին հասանելություն ստանալու մասին դիմում և ստանալ նրան վերաբերող տվյալները[33]:

Օրինակ 12. Տվյալների սուբյեկտ տիկին X-ն իր հետ պայմանագրային հարաբերությունների մեջ գտնվող էլեկտրաէներգետիկական ընկերության հեռախոսային օգնության գծով խորհրդատուի հետ խոսակցության ընթացքում խնդրել է տրամադրել իրեն վերաբերող տվյալներին հասանելիություն: Խորհրդատուն, կասկածներ ունենալով դիմում ներկայացնող անձի ինքնության առնչությամբ, ընկերության համակարգում գեներացնում է մեկանգամյա եզակի ծածկագիր, որն ուղարկվում է օգտատիրոջը՝ հաշիվը բացելիս տրամադրված բջջային հեռախոսահամարին՝ կրկնակի ստուգման համակարգի շրջանակներում, ինչն այս դեպքում պետք է համարվի համաչափ:

3.3 Դիմում ներկայացնող անձի իսկորոշման համաչափության գնահատումը

70. Ինչպես նշվեց վերևը, եթե հսկողն ունի դիմում ներկայացնող անձի ինքնության հարցում կասկածելու հիմնավոր հիմքեր, ապա նա կարող է լրացուցիչ տեղեկություններ պահանջել՝ տվյալների սուբյեկտի ինքնությունը հաստատելու համար: Այնուամենայնիվ, հսկողը պետք է միևնույն ժամանակ ապահովի, որ չհավաքագրի ավելի շատ անձնական տվյալներ, քան անհրաժեշտ է դիմում ներկայացնող անձի իսկորոշման համար: Հետևաբար, հսկողն իրականացնում է համաչափության գնահատում, որի ժամանակ պետք է հաշվի առնվի մշակվող անձնական տվյալների տեսակը (օրինակ՝ տվյալների հատուկ կատեգորիաներ են, թե ոչ), դիմումի բնույթը, դիմումը ներկայացնելու համատեքստը, ինչպես նաև ցանկացած վնաս, որը կարող է առաջանալ տվյալների անօրինական հրապարակումից: Համաչափությունը գնահատելիս անհրաժեշտ է հիշել, որ պետք է խուսափել սահմանազանցող տվյալներ հավաքագրելուց՝ միաժամանակ ապահովելով մշակման անվտանգության համապատասխան մակարդակ:

[32] Նույն տեղում, էջ 14:
[33] Նույն տեղում, էջեր 13-14:

71. Հսկողը պետք է կիրառի իսկորոշման ընթացակարգ՝ իրենց տվյալներին հասանելիություն պահանջող անձանց ինքնության մեջ համոզվելու[34] և հասանելիություն ստանալու մասին դիմումներին՝ ՏՊԸԿ 32-րդ հոդվածին համապատասխան ընթացք տալու ամբողջ ընթացքում մշակման անվտանգությունը, այդ թվում, օրինակ՝ տվյալների սուբյեկտների կողմից լրացուցիչ տեղեկություններ տրամադրելու համար ապահով ուղի ապահովելու համար: Իսկորոշման համար կիրառվող մեթոդը պետք է լինի վերաբերելի, համապատասխան, համաչափ և պահպանի տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքը: Եթե հսկողը ձեռնարկում է տվյալների սուբյեկտի իսկորոշմանն ուղղված այնպիսի միջոցներ, որոնք ծանրացուցիչ են, ապա նա պետք է համարժեք հիմնավորի դա և ապահովի բոլոր հիմնարար սկզբունքների կատարումը, այդ թվում՝ տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքը և տվյալների սուբյեկտների իրավունքների իրացումը դյուրացնելու պարտավորությունը (ՏՊԸԿ 12(2) հոդված):

72. Առցանց միջավայրում իսկորոշման մեխանիզմը կարող է ներառել նույն պարամետրերը, որոնք տվյալների սուբյեկտն օգտագործում է հսկողի կողմից առաջարկվող առցանց ծառայություն մուտք գործելու համար (ՏՊԸԿ 57-րդ ներածական դրույթ)[35]:

73. Գործնականում իսկորոշման ընթացակարգերը հաճախ արդեն առկա են լինում, և հսկողները կարող են այլևս չներդնել լրացուցիչ երաշխիքներ՝ դեպի ծառայություններ չարտոնված մուտքը կանխելու համար: Որպեսզի անձինք կարողանան հասանելիություն ունենալ իրենց հաշիվներում (օրինակ՝ էլեկտրոնային փոստի հաշվում, սոցիալական ցանցերի կամ առցանց խանութների հաշվում) առկա տվյալներին, հսկողները, ամենայն հավանականությամբ, կպահանջեն օգտատիրոջ մուտքանվան և գաղտնաբառի միջոցով մուտքագործում, որը նման դեպքերում պետք է բավարար լինի տվյալների սուբյեկտի իսկորոշման համար[36]: Ավելին, տվյալների սուբյեկտները հաճախ արդեն իսկ իսկորոշված են հսկողի կողմից՝ մինչև պայմանագիր կնքելը կամ մշակման համար նրանց համաձայնությունն ստանալը, և արդյունքում, մշակման գործընթացին մասնակցող շահագրգիռ անձին գրանցելու համար օգտագործվող անձնական տվյալները կարող են օգտագործվել նաև՝ որպես տվյալների սուբյեկտին հասանելիության նպատակներով իսկորոշելու համար ապացույց[37]: Հետևաբար, անհամաչափ կլինի անձը հաստատող փաստաթղթի պատճեն պահանջելն այն դեպքում, երբ դիմում ներկայացնող տվյալների սուբյեկտն արդեն իսկ իսկորոշված է հսկողի կողմից:

---

[34] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 14:

[35] Նույնականացման մեթոդների վերաբերյալ լրացուցիչ ուղղորդման համար տե՛ս Տվյալների արտահոսքի դեպքում ծանուցման օրինակների վերաբերյալ ՏՊԵԽ-ի կողմից 2021 թվականի հունվարի 14-ին ընդունված 01/2021 ուղեցույցը, էջ 30-31, ինչպես նաև Վիրտուալ ձայնային օգնականների վերաբերյալ ՏՊԵԽ-ի 02/2021 ուղեցույցը, տարբերակ 2.0, 2021 թվականի հուլիսի 7, բաժին 3.7:

[36] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 14:

[37] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 14:

74. Պետք է ընդգծել, որ որպես իսկորոշման գործընթացի մաս անձը հաստատող փաստաթղթի պատճենի օգտագործումը ռիսկի տակ է դնում անձնական տվյալների անվտանգությունը և կարող է հանգեցնել չարտոնված կամ անօրինական ճանապարհով մշակման, և, որպես այդպիսին, այն պետք է համարվի անհամաչափ, եթե այն անհրաժեշտ, նպատակահարմար և ազգային իրավունքին համահունչ չէ: Նման դեպքերում հսկողները պետք է ունենան անվտանգության այնպիսի հնարավորություններով համակարգեր, որոնց շնորհիվ նվազեցվում են այդպիսի տվյալներ ստանալու՝ տվյալների սուբյեկտի իրավունքներին և ազատություններին սպառնացող առավել բարձր ռիսկերը: Կարևոր է նաև նշել, որ նույնականացման քարտի միջոցով իսկորոշումն իրականում չի օգնում առցանց միջավայրում (օրինակ՝ կեղծանունների օգտագործմամբ), եթե տվյալ անձը չի կարող որևէ այլ ապացույց, օրինակ՝ օգտվողի հաշվին համապատասխանող լրացուցիչ բնութագրեր ներկայացնել:

75. Հաշվի առնելով այն փաստը, որ շատ կազմակերպություններ (օրինակ՝ հյուրանոցներ, բանկեր, մեքենաների վարձույթով զբաղվող ընկերություններ) պահանջում են իրենց հաճախորդների նույնականացման քարտի պատճենները, դա, ընդհանուր առմամբ, չպետք է համարվի իսկորոշման համար պատշաճ միջոց: Որպես այլընտրանք՝ հսկողը կարող է կիրառել տվյալների սուբյեկտին նույնականացնելու արագ և արդյունավետ անվտանգության միջոց՝ նախկինում իրականացրած իսկորոշման հիման վրա, օրինակ՝ էլեկտրոնային փոստի կամ տեքստային հաղորդագրության միջոցով, որը պարունակում է հաստատման հղումներ, անվտանգության հարցեր կամ հաստատման ծածկագրեր[38]:

76. Անձը հաստատող փաստաթղթի տեղեկությունները, որոնք անհրաժեշտ չեն տվյալների սուբյեկտի ինքնությունը հաստատելու համար, ինչպիսիք են մուտքի և սերիական համարը, ազգությունը, չափսը, աչքերի գույնը, լուսանկարը և մեքենայաընթեռնելի գոտին, կախված յուրաքանչյուր դեպքի գնահատումից, կարող են մինչև դրանք հսկողին ներկայացնելը խմբագրվել կամ թաքցվել տվյալների սուբյեկտի կողմից, բացառությամբ այն դեպքերի, երբ ազգային օրենսդրությամբ պահանջվում է անձը հաստատող փաստաթղթի ամբողջական չխմբագրված պատճենը (տե՛ս ստորև՝ 78-րդ պարբերությունը): Ընդհանուր առմամբ, տրման ամսաթիվը կամ վավերականության ժամկետը, տրամադրող մարմինը և առցանց հաշվի հետ համընկնող ամբողջական անունը բավարար են, որ հսկողն ստուգի ինքնությունը՝ միշտ պայմանով, որ պատճենի իսկությունը, և դիմողի հետ կապն ապահովված է: Լրացուցիչ տեղեկություններ, ինչպիսիք են տվյալների սուբյեկտի ծննդյան ամսաթիվը, կարող են պահանջվել միայն այն դեպքում, երբ սխալ ինքնության ռիսկը դեռևս առկա է, և եթե հսկողը կարող է այն համեմատել արդեն իսկ մշակվող տեղեկությունների հետ:

[38] Տե՛ս նաև «Էլեկտրոնային նույնականացման ու ներքին շուկայում էլեկտրոնային գործարքների համար տրաստային ծառայությունների մասին և 1999/93/ԵՀ հրահանգն ուժը կորցրած ճանաչող» Եվրոպական պառլամենտի և Խորհրդի 2014 թվականի հուլիսի 23-ի թիվ 910/2014 (ԵՄ) կանոնակարգը, որով առաջարկվում են անվտանգ հեռավար նույնականացում ապահովող տարբեր ծառայություններ:

77. Տվյալների ծավալը նվազագույնի հասցնելու սկզբունքը պահպանելու համար հսկողը պետք է տեղեկացնի տվյալների սուբյեկտին այն տեղեկությունների մասին, որոնք անհրաժեշտ չեն, ինչպես նաև անձը հաստատող փաստաթղթի այդ մասերը խմբագրելու կամ թաքցնելու հնարավորության մասին: Նշված դեպքում, եթե տվյալների սուբյեկտը չգիտի կամ ունակ չէ խմբագրելու այդ տեղեկությունները, ապա ցանկալի է, որ այն խմբագրվի հսկողի կողմից՝ փաստաթուղթն ստանալուց հետո, եթե նա ունի այդպիսի հնարավորություն՝ հաշվի առնելով այդ հանգամանքներում հսկողին հասանելի միջոցները:

Օրինակ 13. Օգտվող տիկին Y-ն առցանց խանութում ստեղծել է գաղտնաբառով պաշտպանված հաշիվ՝ տրամադրելով իր էլեկտրոնային փոստի հասցեն և (կամ) օգտանունը: Հետագայում, հաշվի սեփականատերը խնդրում է հսկողին տրամադրել տեղեկություններ այն մասին, թե արդյոք նա մշակում է իր անձնական տվյալները, և եթե այո, ապա տրամադրել դրանց հասանելիություն՝ 15-րդ հոդվածում նշված շրջանակներում: Հսկողը պահանջում է դիմում ներկայացնող անձի նույնականացման փաստաթուղթը՝ նրա ինքնությունը հաստատելու համար: Այս դեպքում հսկողի գործողությունն անհամաչափ է և հանգեցնում է անհարկի տվյալների հավաքագրման:

Այնուամենայնիվ, դիմում ներկայացնող անձի ինքնությունը հաստատելու, և միաժամանակ անհարկի տվյալների հավաքագրումը կանխելու նպատակով հսկողը կարող է նրանից պահանջել իսկորոշում անցնել հաշիվ մուտք գործելու կամ նրան անվտանգության հարցեր (ոչ անպարկեշտ) տալու միջոցով, որոնց պատասխանը պետք է իմանա միայն տվյալների սուբյեկտը, կամ օգտագործել բազմագործոն նույնականացում, որը կազմաձևվել է տվյալների սուբյեկտի կողմից իր հաշիվը գրանցելուց, կամ օգտագործել տվյալների սուբյեկտին պատկանող այլ առկա կապի միջոցներ, ինչպիսիք են էլեկտրոնային փոստի հասցեն կամ հեռախոսահամարը՝ մուտքի գաղտնաբառն ուղարկելու համար:

Օրինակ 14. Բանկի հաճախորդը՝ պարոն Y-ը, պլանավորում է վերցնել սպառողական վարկ: Այդ նպատակով պարոն Y-ը դիմում է բանկի մասնաճյուղ՝ իր վարկունակությունը գնահատելու համար անհրաժեշտ տեղեկությունները, այդ թվում՝ իր անձնական տվյալներն ստանալու համար: Տվյալների սուբյեկտի ինքնությունն ստուգելու համար խորհրդատուն դիմում է նրան վերջինիս ինքնությունը հաստատող՝ նոտարական կարգով վավերացված փաստաթուղթը տրամադրելու խնդրանքով, որպեսզի կարողանա նրան տրամադրել պահանջվող տեղեկությունները:
Հսկողը չպետք է պահանջի ինքնությունը հաստատող՝ նոտարական կարգով վավերացված փաստաթուղթ, բացառությամբ այն դեպքերի, երբ դա անհրաժեշտ է, նպատակահարմար և համահունչ է ազգային իրավունքին (օրինակ, երբ անձը ժամանակավորապես չունի անձը հաստատող որևէ փաստաթուղթ, և տվյալների սուբյեկտի ինքնության հաստատումը պահանջվում է ազգային իրավունքով՝ իրավական ակտի կատարման համար): Այս գործելակերպը դիմում ներկայացնող անձանց համար առաջացնում է լրացուցիչ ծախսեր և սահմանազանցող բեռ է դնում տվյալների սուբյեկտների վրա՝ խոչընդոտելով նրանց հասանելիություն ունենալու իրավունքի իրացումը:

78. Չհակասելով վերը նշված ընդհանուր սկզբունքներին՝ որոշ հանգամանքներում անձը հաստատող փաստաթղթի հիման վրա իսկորոշումը կարող է հիմնավորված և համաչափ միջոց լինել, մասնավորապես հատուկ կատեգորիաների անձնական տվյալներ մշակող կամ տվյալների մշակում իրականացնող անձանց համար, ինչը կարող է վտանգ ներկայացնել տվյալների սուբյեկտի համար (օրինակ՝ բժշկական կամ առողջական վիճակի մասին տեղեկություններ): Այնուամենայնիվ, միևնույն ժամանակ պետք է նկատի ունենալ, որ ազգային իրավունքի որոշ դրույթներով սահմանափակումներ են նախատեսվում պաշտոնական փաստաթղթերում, այդ թվում՝ անձի ինքնությունը հաստատող փաստաթղթերում պարունակվող տվյալների մշակման նկատմամբ (նաև ՏՊԸԿ 87-րդ հոդվածի հիման վրա): Այս փաստաթղթերից տվյալների մշակման նկատմամբ սահմանափակումները կարող են վերաբերել, մասնավորապես, նույնականացման քարտերի արտապատկերմանը կամ պատճենահանմանը կամ անձը հաստատող պաշտոնական համարների մշակմանը[39]:

[39] Այս կապակցությամբ մի քանի անդամ պետություններ նման սահմանափակում են մտցրել իրենց ազգային դրույթներում՝ նշելով, որ, օրինակ՝ նույնականացման քարտերի պատճենահանումն օրինական է միայն այն դեպքում, եթե դա ուղղակիորեն բխում է իրավական ակտի դրույթներից:

79. Հաշվի առնելով վերոնշյալը, երբ պահանջվում է անձը հաստատող փաստաթուղթ (և դա համահունչ է ինչպես ազգային իրավունքին, այնպես էլ ՏՊԸԿ համաձայն հիմնավորված և համաչափ է), հսկողը պետք է երաշխիքներ սահմանի՝ անձը հաստատող փաստաթղթի անօրինական ճանապարհով մշակումը կանխելու համար: Չնայած անձը հաստատող փաստաթղթի իսկորոշման վերաբերյալ գործող ազգային դրույթներին՝ դա կարող է ներառել անձը հաստատող փաստաթուղթը պատճենելուց կամ տվյալների սուբյեկտի ինքնության հաջող իսկորոշումից անմիջապես հետո դրա պատճենը ջնջելուց ձեռնպահ մնալը: Դա պայմանավորված է նրանով, որ անձը հաստատող փաստաթղթի պատճենի հետագա պահպանումը կարող է հավասարազոր լինել նպատակների սահմանափակման և պահպանման ժամկետի սահմանափակման սկզբունքների (ՏՊԸԿ 5(1)(բ) և (ե) հոդված), ինչպես նաև ազգային նույնականացման համարի մշակմանը վերաբերող ազգային օրենսդրության (ՏՊԸԿ 87-րդ հոդված) խախտման: ՏՊԵԽ-ը, որպես լավագույն գործելակերպ, առաջարկում է, որ հսկողը, անձը հաստատող փաստաթուղթն ստուգելուց հետո, նշում կատարի, որ, օրինակ՝ «Նույնականացման քարտը ստուգված է»՝ նույնականացման քարտերի պատճենների անհարկի պատճենումից կամ պահպանումից խուսափելու համար:

3.4 Երրորդ անձանց/վստահված անձանց միջոցով ներկայացված դիմումները

80. Թեև հասանելիություն ունենալու իրավունքն ընդհանուր առմամբ իրացվում է տվյալների սուբյեկտների կողմից, քանի որ դա նրանց է վերաբերում, այնուամենայնիվ, երրորդ անձը կարող է դիմում ներկայացնել տվյալների սուբյեկտի անունից: Սա կարող է, *ի թիվս այլնի*, վերաբերել անչափահասների անունից վստահված անձի կամ օրինական խնամակալների, ինչպես նաև առցանց պորտալների միջոցով այլ կազմակերպությունների միջոցով դիմում ներկայացնելուն: Որոշ հանգամանքներում հասանելիություն ունենալու իրավունքն իրացնելու լիազորություն ունեցող անձի ինքնությունը, ինչպես նաև տվյալների սուբյեկտի անունից գործելու թույլտվությունը կարող են պահանջել ստուգում, եթե դա նպատակահարմար և համաչափ է (տե՛ս վերը նշված 3.3 բաժինը)[40]: Հարկ է հիշեցնել, որ անձնական տվյալները որևէ մեկին հասանելի դարձնելը, ով չունի դրանց հասանելիություն ունենալու իրավունքը, կարող է համարվել անձնական տվյալների խախտում[41]:

[40] Հասանելիություն ունենալու իրավունքի իրացման ժամկետների համար, երբ հսկողը լրացուցիչ տեղեկություններ ստանալու կարիք ունի, տե՛ս 157-րդ պարբերությունը:
[41] ՏՊԸԿ 4(12) հոդված:

81. Ընդ որում պետք է հաշվի առնել իրավական ներկայացուցչությունը (օրինակ՝ լիազորագրերը) կարգավորող ազգային օրենքները, որոնցով հնարավոր է սահմանել հատուկ պահանջներ՝ տվյալների սուբյեկտի անունից դիմում ներկայացնելու թույլտվությունն ապացուցելու համար, քանի որ այս հարցը չի կարգավորվում ՏՊԸԿ-ով: Հաշվետվողականության սկզբունքին, ինչպես նաև տվյալների պաշտպանության այլ սկզբունքներին համապատասխան՝ հսկողները պետք է կարողանան ապացուցել տվյալների սուբյեկտի անունից դիմում ներկայացնելու և պահանջվող տեղեկություններն ստանալու համապատասխան թույլտվության առկայությունը, բացառությամբ այն դեպքերի, երբ ազգային իրավունքը տարբերվում է (օրինակ՝ ազգային իրավունքով նախատեսվում են հատուկ կանոններ՝ կապված փաստաբանների վստահելիության հետ), որի արդյունքում հսկողին թույլ է տրվում ստուգել վստահված անձի ինքնությունը (օրինակ՝ փաստաբանների դեպքում ստուգվում է Փաստաբանների ասոցիացիայում նրանց ընդգրկվածությունը): Հետևաբար, առաջարկվում է այս առնչությամբ հավաքել համապատասխան փաստաթղթեր՝ կապված դիմում ներկայացնող ֆիզիկական անձի ինքնության հաստատմանը վերաբերող՝ նախկինում նշված ընդհանուր կանոնների հետ, և եթե հսկողը հիմնավոր կասկածներ ունի տվյալների սուբյեկտի անունից հանդես եկող անձի ինքնության առնչությամբ, ապա նա լրացուցիչ տեղեկություններ է պահանջում՝ այդ անձի ինքնությունը հաստատելու համար:

82. Թեև մահացած անձանց անձնական տվյալների հասանելիություն ունենալու իրավունքի իրացումը հավասարազոր է տվյալների սուբյեկտից բացի երրորդ անձի կողմից հասանելիության մեկ այլ օրինակի, 27-րդ ներածական դրույթում նշվում է, որ ՏՊԸԿ-ն չի կիրառվում մահացած անձանց անձնական տվյալների նկատմամբ: Հետևաբար, հարցը կարգավորվում է ազգային իրավունքով, և անդամ պետությունները կարող են նախատեսել մահացած անձանց անձնական տվյալների մշակման կանոններ: Այնուամենայնիվ, պետք է նկատի ունենալ, որ տվյալները, բացի դրանից, կարող են վերաբերել կենդանի երրորդ անձանց, օրինակ՝ մահացած անձի նամակագրությանը հասանելիություն ստանալու համատեքստում: Այդ տվյալների գաղտնիությունը դեռ պետք է պաշտպանվի:

3.4.1 Երեխաների անունից հասանելիություն ունենալու իրավունքի իրացումը

83. Երեխաներն արժանի են իրենց անձնական տվյալների հատուկ պաշտպանության, քանի որ նրանք կարող են ավելի քիչ տեղեկացված լինել անձնական տվյալների մշակման առնչությամբ իրենց իրավունքների հետ կապված ռիսկերի, հետևանքների և երաշխիքների մասին[42]: Երեխային ուղղված ցանկացած տեղեկություն և հաղորդակցություն, որի դեպքում մշակվում են երեխայի անձնական տվյալները, պետք է լինեն հստակ և պարզ լեզվով, որպեսզի երեխան կարողանա հեշտությամբ հասկանալ:[43]

84. Երեխաներն ինքնին հանդիսանում են տվյալների սուբյեկտներ և, որպես այդպիսին, հասանելիություն ունենալու իրավունքը պատկանում է երեխային: Կախված երեխայի հասունությունից և կարողությունից՝ նրան կարող է անհրաժեշտ լինել երրորդ անձ, օրինակ՝ ծնողական իրավունքներ ունեցող անձինք, որոնք հանդես կգան նրա անունից:

85. Երեխայի լավագույն շահերը պետք է լինեն երեխաների հասանելիություն ունենալու իրավունքի իրացման առնչությամբ կայացված բոլոր որոշումների հիմնական նկատառումը, մասնավորապես, երբ հասանելիություն ունենալու իրավունքն իրացվում

է երեխայի անունից, օրինակ՝ ծնողական լիազորություն ունեցող անձանց կողմից:

86. Հաշվի առնելով ՏՊԸԿ-ով նախատեսված՝ երեխաների անձնական տվյալների հատուկ պաշտպանությունը՝ հսկողը ձեռնարկում է համապատասխան միջոցներ՝ չլիազորված անձին անչափահասի անձնական տվյալների ցանկացած հրապարակումից խուսափելու համար (այս առումով տե՛ս նաև վերը նշված 3.4 բաժինը):

87. Վերջապես, երեխայի անունից գործելու՝ ծնողական իրավունքներ ունեցող անձի իրավունքը չպետք է շփոթել տվյալների պաշտպանության մասին իրավունքից դուրս գործող դեպքերի հետ, երբ ազգային օրենսդրությամբ ծնողական իրավունքներ ունեցող անձին իրավունք է վերապահվում՝ դիմելու երեխայի վերաբերյալ տեղեկությունների համար և ստանալու դրանք (օրինակ՝ դպրոցում երեխայի առաջադիմության վերաբերյալ):

3.4.2 Երրորդ անձի կողմից տրամադրված պորտալների/ալիքների միջոցով հասանելիություն ունենալու իրավունքի իրացումը

88. Գոյություն ունեն ծառայություններ մատուցող ընկերություններ, որոնք տվյալների սուբյեկտներին հնարավորություն են ընձեռում պորտալի միջոցով ներկայացնել հասանելիություն ստանալու մասին դիմումներ: Տվյալների սուբյեկտը մուտք է գործում պորտալ և ստանում է պորտալին հասանելիություն, որի միջոցով նա կարողանում է ներկայացնել, օրինակ՝ հասանելիություն ստանալու մասին դիմում, պահանջել տվյալների ուղղում կամ տվյալների ոչնչացում տարբեր հսկողներից: Երրորդ անձի կողմից տրամադրված պորտալների օգտագործումից առաջանում են տարբեր հարցեր:

89. Առաջին խնդիրը, որը հսկողները պետք է լուծեն նման դեպքերի բախվելիս, այն է, որ պետք է ապահովեն, որ երրորդ անձը տվյալների սուբյեկտի անունից գործի իրավաչափ, քանի որ անհրաժեշտ է համոզվել, որ ոչ մի տվյալ չի հրապարակվում չլիազորված անձանց:

90. Բացի դրանից, հսկողը, որը ստանում է այդ պորտալի միջոցով ներկայացված դիմումը, միշտ պետք է ժամանակին ընթացք տա այդ դիմումին[44]: Այնուամենայնիվ, հսկողը պարտավոր չէ ուղղակիորեն պորտալում տրամադրել տվյալներ՝ ՏՊԸԿ 15-րդ հոդվածի համաձայն, եթե նա, օրինակ՝ հաստատում է, որ անվտանգության միջոցները բավարար չեն, կամ նպատակահարմար կլինի օգտագործել տվյալների սուբյեկտին տվյալների հրապարակման մեկ այլ եղանակ: Նման դեպքերում, երբ հսկողն ունի այլ ընթացակարգեր՝ հասանելիություն ստանալու մասին դիմումներն արդյունավետ և ապահով կերպով լուծելու համար, հսկողը կարող է տրամադրել պահանջվող տեղեկություններն այդ ընթացակարգերի միջոցով:

[42] ՏՊԸԿ 38-րդ ներածական դրույթ:Ինչպես նախատեսված է ՏՊԸԿ աշխատանքային ծրագրում, դրա նպատակը երեխաների տվյալների վերաբերյալ ուղղություն ցույց տալն է: Ակնկալվում է, որ այդ փաստաթուղթն առավել շատ ուղղորդում կտրամադրի այն պայմանների վերաբերյալ, որոնց համաձայն երեխան կարող է իրացնել հասանելիություն ունենալու իր իրավունքը, և ծնողական իրավունքներ ունեցող անձը կարող է երեխայի անունից իրացնել հասանելիություն ունենալու իրավունքը:

[43] ՏՊԸԿ 58-րդ ներածական դրույթ: 2016/679 կանոնակարգին համապատասխան համաձայնության վերաբերյալ ՏՊԵԽ-ի 05/2020 ուղեցույց, բաժին 7:

[44] Հասանելիություն ունենալու իրավունքի իրացման ժամկետների համար, երբ հսկողը լրացուցիչ տեղեկություններ ստանալու կարիք ունի, տե՛ս 157-րդ պարբերությունը:

4 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՈՒՆԵՆԱԼՈՒ ԻՐԱՎՈՒՆՔԻ ՇՐՋԱՆԱԿԸ ԵՎ ԱՅՆ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐՆ ՈՒ ՏԵՂԵԿՈՒԹՅՈՒՆՆԵՐԸ, ՈՐՈՆՑ ԴԱ ՎԵՐԱԲԵՐՈՒՄ Է

91. Սույն բաժինը նպատակ ունի լույս սփռել անձնական տվյալների սահմանման վրա (4.1) և հստակեցնել այն տեղեկությունների շրջանակը, որոնք ընդհանուր առմամբ կարգավորվում են հասանելիություն ունենալու իրավունքով (4.2 և 4.3): Հատկանշական է, որ անձնական տվյալների հասկացության շրջանակը և, հետևաբար, անձնական տվյալների և մյուս տվյալների միջև տարբերակումը կազմում է հսկողի կողմից կատարվող գնահատման անբաժանելի մասը, որը միտված է վերհանելու այն տվյալների շրջանակը, որին տվյալների սուբյեկտն իրավունք ունի ստանալու հասանելիություն[45]:

92. Որպես նախնական նկատառում՝ պետք է հիշել, որ հասանելիություն ունենալու իրավունքը կարող է իրացվել միայն ՏՊԸԿ նյութական և տարածքային կիրառման շրջանակում գտնվող անձնական տվյալների մշակման առնչությամբ: Հետևաբար, այն անձնական տվյալները, որոնք չեն մշակվում ավտոմատացված միջոցներով, կամ որոնք չեն հանդիսանում կամ նախատեսված չեն դառնալու հաշվառման համակարգի մաս՝ ՏՊԸԿ 2(1) հոդվածի համաձայն կա՛մ մշակվում են ֆիզիկական անձի կողմից զուտ անձնական կա՛մ կենցաղային գործունեության ընթացքում, չեն կարգավորվում հասանելիություն ունենալու իրավունքով:

4.1 Անձնական տվյալների սահմանումը

93. ՏՊԸԿ 15(1) և (3) հոդվածը վերաբերում է համապատասխանաբար «*անձնական տվյալներին*» և «*մշակվող անձնական տվյալներին*»: Հետևաբար, հասանելիություն ունենալու իրավունքի շրջանակը նախևառաջ որոշվում է ՏՊԸԿ 4(1) հոդվածով սահմանված անձնական տվյալների հասկացության շրջանակով[46]: Անձնական տվյալների հասկացությունն արդեն եղել է 29-րդ հոդվածով սահմանված աշխատանքային խմբի[47] մի քանի փաստաթղթերի[48] առարկա և մեկնաբանվել է ԵՄԱԴ-ի կողմից, այդ թվում՝ 95/46/ԵՀ հրահանգի 12-րդ հոդվածի համաձայն հասանելիություն ունենալու իրավունքի համատեքստում:

[45] Ներկառուցված անձեռնմխելության սկզբունքին համապատասխան՝ այդ վերլուծությունը հանդիսանում է տվյալների պաշտպանության սկզբունքների և տվյալների սուբյեկտի իրավունքների պաշտպանությանն ուղղված համապատասխան միջոցների ու երաշխիքների գնահատման մաս, որն իրականացվում է «*մշակման միջոցների որոշման և հենց մշակման պահին*», օրինակ՝ պատասխանի տրամադրման ժամանակի կրճատումը, երբ տվյալների սուբյեկտներն իրացնում են իրենց իրավունքները, կարող է լինել ցուցանիշներից մեկը: Լրացուցիչ բացատրությունների համար տե՛ս Տվյալների՝ հայեցակարգային և լռելյայն պաշտպանության մասին 25-րդ հոդվածի վերաբերյալ 4/2019 ուղեցույց:

[46] ՏՊԸԿ 4(1) հոդվածի համաձայն՝ ««անձնական տվյալներ» նշանակում է նույնականացված կամ նույնականացման ենթական ֆիզիկական անձին («տվյալների սուբյեկտին») վերաբերող ցանկացած տեղեկություն. նույնականացման ենթակա ֆիզիկական անձն այն անձն է, որը կարող է ուղղակիորեն կամ անուղղակիորեն նույնականացվել, մասնավորապես՝ նույնականացուցիչի՝ անունի, նույնականացման համարի, գտնվելու վայրի վերաբերյալ տվյալների, առցանց նույնականացուցիչի կամ այդ անձի ֆիզիկական, ֆիզիոլոգիական, գենետիկ, մտավոր, տնտեսական, մշակութային կամ սոցիալական ինքնությանը բնորոշ մեկ կամ մի քանի գործոնների միջոցով:»

[47] 29-րդ հոդվածով սահմանված աշխատանքային խումբը (29-րդ հոդվածով սահմանված աշխատանքային խումբ), ՏՊԵԽ-ի իրավանախորդը, անկախ եվրոպական աշխատանքային խումբ է, որը մինչև 2018 թվականի մայիսի 25-ը (մինչև ՏՊԸԿ կիրառման մեջ մտնելը) զբաղվում էր անձեռնմխելիության և անձնական տվյալների պաշտպանության հետ կապված հարցերով:

[48] Օրինակ՝ 2016/679 կանոնակարգի նպատակներով ավտոմատացված անհատական որոշումների կայացման, այդ թվում՝ պրոֆիլավորման վերաբերյալ աշխատանքային խմբի 251, rev01 ուղեցույց, էջ 19, ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի 29 ուղեցույց, էջ 9:

94. 29-րդ հոդվածով սահմանված աշխատանքային խումբը գտել է, որ 95/46/ԵՀ հրահանգում անձնական տվյալների սահմանումն «*արտացոլում է եվրոպացի օրենսդրի մտադրությունը՝ ընդլայնելու «անձնական տվյալների» հասկացությունը*»[49]: ՏՊԸԿ համաձայն՝ սահմանումը դեռևս վերաբերում է «*նույնականացված կամ նույնականացման ենթակա ֆիզիկական անձին վերաբերող ցանկացած տեղեկության*»: Բացի հիմնական անձնական տվյալներից՝ անունից և հասցեից, հեռախոսահամարից և այլ տվյալներից՝ այս սահմանման մեջ կարող են մտնել անսահմանափակ, տարատեսակ տվյալներ, այդ թվում՝ բժշկական եզրակացություններ, գնումների պատմություն, վարկունակության ցուցանիշներ, հաղորդակցության բովանդակություն և այլն: Անձնական տվյալների լայն սահմանման լույսի ներքո հսկողի կողմից այդ սահմանման սահմանափակող գնահատումը կհանգեցնի անձնական տվյալների սխալ դասակարգման[50] և, ի վերջո, հասանելիություն ունենալու իրավունքի խախտման:

95. *Թիվ C-141/12 և թիվ C-372/12 միացված գործերով*[51] ԵՄԱԴ-ը վճռել է, որ հասանելիություն ունենալու իրավունքը ներառում է արձանագրություններում պարունակվող անձնական տվյալները, այն է՝ «*դիմողի անունը, ծննդյան ամսաթիվը, ազգությունը, սեռը, էթնիկ պատկանելությունը, կրոնն ու լեզուն*» «*և, հարկ եղած դեպքում, արձանագրության մեջ պարունակվող իրավական վերլուծության տվյալները*», սակայն ոչ բուն իրավական վերլուծությունը[52]: Իրավական վերլուծությունն այս համատեքստում ինքնին ենթակա չէր դրա ճշգրտության մասով տվյալների սուբյեկտի կողմից ստուգման կամ ուղղման: Ավելին, իրավական վերլուծության հասանելիության ապահովումը չի ծառայում անձեռնմխելիության երաշխավորման նպատակին, այլ ապահովում է վարչական փաստաթղթերի հասանելիությունը:

96. *Նովակի գործով* [Nowak][53] ԵՄԱԴ-ն առավել լայն վերլուծություն է կատարել և պարզել, որ մասնագիտական քննության ժամանակ թեկնածուի կողմից ներկայացված գրավոր պատասխանները և այդ պատասխանների առնչությամբ քննող անձի ցանկացած դիտարկում կազմում են քննության թեկնածուին վերաբերող անձնական տվյալներ: Առավել կոնկրետ՝ այդ սուբյեկտիվ տեղեկություններն անձնական տվյալներ են «*կարծիքների և գնահատականների տեսքով, եթե դրանք «վերաբերում են» տվյալների սուբյեկտին*»[54]՝ ի տարբերություն քննության հարցերի, որոնք անձնական տվյալներ չեն համարվում[55]: Այսպիսով, համատեքստի գնահատումը պետք է լույս սփռի այն ազդեցության կամ արդյունքի վրա, որը տեղեկությունները կարող են թողնել անձի վրա, հետևաբար՝ հասանելիություն ունենալու իրավունքի շրջանակի վրա:

[49] 29-րդ հոդվածով սահմանված աշխատանքային խմբի 29 կարծիք անձնական տվյալների հասկացության վերաբերյալ, էջ 4:

[50] որպես նույնականացված կամ նույնականացման ենթակա ֆիզիկական անձին չվերաբերվող տեղեկություններ:

[51] ԵՄԱԴ, *թիվ C-141/12 և թիվ C-372/12 միացված գործեր, Ուայէս-ն ընդդեմ Ներգաղթի, ինտեգրման և ապաստանի հարցերով նախարարի, ինչպես նաև Ներգաղթի, ինտեգրման և ապաստանի հարցերով նախարարն ընդդեմ ԷՄ և ԷՄ-ի գործ* [YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S], 2014 թվականի հուլիսի 17:

[52] ԵՄԱԴ, *թիվ* C-141/12 և *թիվ* C-372/12 միացված գործեր, *Ուայէս-ը և այլք գործ* [YS and Others], պարբերություններ 38 և 48:

[53] ԵՄԱԴ, գործ թիվ C-434/16, *Պիտեր Նովակն ընդդեմ Տվյալների պաշտպանության հարցերով հանձնակատարի գործ* [Peter Nowak v Data Protection Commissioner], 2017 թվականի դեկտեմբերի 20:

[54] ԵՄԱԴ, գործ թիվ C 434/16, *Նովակի գործ*, պարբերություններ 34- 35:

[55] ԵՄԱԴ, գործ թիվ C-434/16, *Նովակի գործ*, պարբերություն 58:

Օրինակ 15. Անձը հարցազրույց է անցնում ընկերությունում: Այդ նպատակով դիմորդն ինքնակենսագրական և դիմում-նամակ է ներկայացնում: Հարցազրույցի ժամանակ ՄՌԿ աշխատակիցը համակարգչի վրա գրառումներ է կատարում՝ հարցազրույցը փաստաթղթավորելու համար: Հարցազրույցից հետո դիմորդը, որպես տվյալների սուբյեկտ, դիմում է իրեն վերաբերող անձնական տվյալներին հասանելիություն ապահովելու խնդրանքով, որոնք ընկերությունը՝ որպես հսկող, հավաքագրել է աշխատանքի ընդունելու ընթացակարգի ժամանակ:

Հսկողը պարտավոր է տվյալների սուբյեկտին տրամադրել այն անձնական տվյալները, որոնք տվյալների սուբյեկտն ինքնակամ ներկայացրել էր իր ինքնակենսագրականում և դիմում-նամակում: Ավելին, հսկողը պետք է տվյալների սուբյեկտին տրամադրի հարցազրույցի ամփոփագիրը, այդ թվում՝ տվյալների սուբյեկտի վարքագծի վերաբերյալ սուբյեկտիվ դիտարկումները, որոնք ՄՌԿ աշխատակիցը գրի է առել հարցազրույցի ժամանակ՝ ազգային օրենսդրության համաձայն ցանկացած բացառության հաշվառմամբ և ՏՊԸԿ 23-րդ հոդվածին համապատասխան:

97. Այսպիսով, ելնելով գործի կոնկրետ փաստերից, հասանելիություն ստանալու մասին կոնկրետ դիմումը գնահատելիս, *ի թիվս այլնի*, հսկողները պետք է տրամադրեն հետևյալ տեսակի տվյալները՝ չհակասելով ՏՊԸԿ 15(4) հոդվածը.

- հատուկ կատեգորիայի անձնական տվյալները՝ ՏՊԸԿ 9-րդ հոդվածի համաձայն.
- դատվածություններին և կատարված իրավախախտումներին վերաբերող անձնական
- տվյալները՝ ՏՊԸԿ 10-րդ հոդվածի համաձայն.
- տվյալների սուբյեկտի կողմից գիտակցաբար և ակտիվորեն տրամադրված տվյալները (օրինակ՝ ձևաթղթերի միջոցով ներկայացված հաշվի տվյալները, հարցաթերթիկի պատասխանները)[56].
- ծառայության կամ սարքի օգտագործման արդյունքում տվյալների սուբյեկտի կողմից տրամադրված՝ դիտարկվող տվյալները կամ չմշակված տվյալները (օրինակ՝ միացված օբյեկտների կողմից մշակված տվյալները, գործարքների պատմությունը, ակտիվության մատյանները, ինչպիսիք են մուտք գործելու մատյանները, կայքի օգտագործման պատմությունը, որոնման գործողությունները, գտնվելու վայրի վերաբերյալ տվյալները, կտացցնելու ակտիվությունը, անձի վարքագծի եզակի կողմերը, ինչպիսիք են ձեռագիրը, ստեղնաշարի հարվածները, քայլելու կամ խոսելու հատուկ ձևը)[57].
- տվյալներ, որոնք ավելի շուտ ստացվում են մյուս տվյալներից, քան ուղղակիորեն տրամադրվում են տվյալների սուբյեկտի կողմից (օրինակ՝ վարկային գծի միջոցների օգտագործման հարաբերակցությունը, տվյալների սուբյեկտների ընդհանուր հատկանիշների վրա հիմնված դասակարգումը, փոստային ինդեքսից ստացված բնակության երկիրը)[58].

---

[56] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 9:

[57] Անձնական տվյալներ հասկացության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի 4/2007 կարծիք, էջ 8:

[58] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ ուղեցույց, էջեր 10-11:

- տվյալներ, որոնք ավելի շուտ դուրս են բերվում մյուս տվյալներից, քան ուղղակիորեն տրամադրվում են տվյալների սուբյեկտի կողմից (օրինակ՝ վարկային միավոր շնորհելու կամ փողերի լվացման դեմ պայքարի կանոնները կատարելու, ալգորիթմների արդյունքները, առողջական վիճակի գնահատման արդյունքները կամ անհատականացման կամ առաջարկությունների գործընթացը պահպանելու համար)[59].
- կեղծանունացված տվյալներ՝ ի տարբերություն անանունացված տվյալների (տե՛ս նաև այդ ուղեցույցի 3-րդ բաժինը):

Օրինակ 16. Այն տարրերը, որոնք հիմք են հանդիսացել, օրինակ՝ աշխատողի առաջխաղացման, աշխատավարձի բարձրացման կամ նոր աշխատանքի նշանակման վերաբերյալ որոշում կայացնելու համար (օրինակ՝ տարեկան կատարողականի գնահատումները, վերապատրաստում անցնելու դիմումները, գրավոր նկատողությունները, վարկանիշը, աշխատանքում առաջխաղացման հնարավորությունները), համարվում են տվյալ աշխատողին վերաբերող անձնական տվյալներ: Ուստի, տվյալների սուբյեկտը կարող է հասանելիություն ստանալ այդ տարրերին՝ ներկայացնելով դիմում և պահպանելով ՏՊԸԿ 15(4) հոդվածը, եթե, օրինակ՝ անձնական տվյալները վերաբերում են նաև մեկ այլ անձի (օրինակ՝ մեկ այլ աշխատողի ինքնությունը կամ նրա ինքնությունը բացահայտող տարրերը, ում կատարողականի վերաբերյալ հավաստումներն ընդգրկված են տարեկան կատարողականի գնահատման մեջ, կարող է սահմանափակվել՝ ՏՊԸԿ 15(4) հոդվածի համաձայն, և, հետևաբար, հնարավոր է, որ դրանք հնարավոր չլինի փոխանցել տվյալների սուբյեկտին՝ նշված աշխատողի իրավունքներն ու ազատությունները պաշտպանելու համար: Այնուամենայնիվ, ազգային աշխատանքային իրավունքի դրույթները կարող են կիրառվել, օրինակ՝ աշխատողների կողմից անձնակազմի փաստաթղթերին հասանելիության դեպքում կամ կարող են կիրառվել այլ ազգային դրույթներ, որոնք վերաբերում են մասնագիտական գաղտնիքին: Բոլոր դեպքերում ազգային իրավունքով նախատեսված՝ տվյալների սուբյեկտի հասանելիություն ունենալու իրավունքի (կամ այլ իրավունքների) իրացման այդ սահմանափակումները պետք է համապատասխանեն ՏՊԸԿ 23-րդ հոդվածի պայմաններին (տե՛ս 6.4 բաժինը):

98. Վերոնշյալ անձնական տվյալների ոչ սպառիչ ցանկից, որոնք կարող են տրամադրվել տվյալների սուբյեկտին հասանելիություն ստանալու մասին դիմումների դեպքում, կարելի է կատարել մի շարք նկատառումներ: Վերոնշյալից ակնհայտ է, որ հսկողն անձնական տվյալներին հասանելիություն ապահովելիս չի կարող տարբերակել թղթային ֆայլերում պարունակվող և էլեկտրոնային եղանակով պահվող տվյալների միջև, եթե դրանք գտնվում են ՏՊԸԿ գործողության շրջանակում: Այլ կերպ ասած, անձնական տվյալները, որոնք պարունակվում են թղթային ֆայլերում՝ որպես հաշվառման համակարգի մաս, կամ այն անձնական տվյալները, որոնք նախատեսված են, որ կազմեն այդ համակարգի մաս, կարգավորվում են հասանելիություն ունենալու իրավունքով այնպես, ինչպես համակարգչի հիշողության մեջ պահվող անձնական տվյալները, օրինակ՝ երկուական ծածկագրի կամ տեսաերիզների միջոցով:

[59] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ ուղեցույց, էջեր 10-11, 29-րդ հոդվածով սահմանված աշխատանքային խումբ, WP 251 rev.01, 2018 թվականի փետրվարի 6, ՏՊԵԽ-ի կողմից հաստատված՝ 2016/679 կանոնակարգի նպատակներով ավտոմատացված անհատական որոշումների կայացման, այդ թվում՝ պրոֆիլավորման վերաբերյալ ուղեցույց (այսուհետ՝ ՏՊԵԽ-ի կողմից հաստատված՝ Ավտոմատացված անհատական որոշումների կայացման, այդ թվում՝ պրոֆիլավորման վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց), էջեր 9-10:

99. Ավելին, ինչպես տվյալների սուբյեկտի իրավունքների մեծ մասը, այնպես էլ հասանելիություն ունենալու իրավունքը ներառում են ինչպես դուրս բերված, այնպես էլ ստացված տվյալներ, այդ թվում՝ ծառայություններ մատուցողի կողմից ստեղծված անձնական տվյալներ, մինչդեռ տվյալների տեղափոխելիության իրավունքը ներառում է միայն տվյալների սուբյեկտի կողմից տրամադրված տվյալները[60]: Հետևաբար, հասանելիություն ստանալու մասին դիմումի դեպքում և ի տարբերություն տվյալների տեղափոխելիության մասին դիմումի, տվյալների սուբյեկտին պետք է տրամադրվեն ոչ միայն հսկողին տրամադրված անձնական տվյալները՝ այդ տվյալների առնչությամբ հետագա վերլուծություն կամ գնահատում կատարելու նպատակով, այլ նաև ցանկացած այդպիսի լրացուցիչ վերլուծության կամ գնահատման արդյունքը:

100. Կարևոր է նաև հիշել, որ կան տեղեկություններ, ինչպես օրինակ՝ անանուն տվյալներ[61], որոնք ուղղակիորեն կամ անուղղակիորեն չեն վերաբերում նույնականացման ենթակա անձին և, հետևաբար, ներառված չեն ՏՊԸԿ շրջանակներում: Օրինակ՝ սերվերի գտնվելու վայրը, որի վրա մշակվում են տվյալների սուբյեկտի անձնական տվյալները, չի համարվում անձնական տվյալ: Տարբերակում մտցնելը կարող է բարդ լինել, և հսկողի մոտ կարող է հարց առաջանալ, թե ինչպես հստակ տարանջատել անձնական և ոչ անձնական տվյալները, մասնավորապես՝ տվյալների խառը հավաքածուները: Նման դեպքում կարող է օգտակար լինել տարանջատել տվյալների խառը հավաքածուները, որոնցում անձնական և ոչ անձնական տվյալներն անքակտելիորեն փոխկապված են, և այն տվյալները, որոնք անքակտելիորեն փոխկապված չեն: Անձնական և ոչ անձնական տվյալները կարող են անքակտելիորեն փոխկապված լինել տվյալների խառը հավաքածուներում և ընդհանուր առմամբ ընկնել այն տվյալների սուբյեկտի հասանելիություն ունենալու իրավունքի շրջանակներում, որին վերաբերում են անձնական տվյալները[62]: Այլ դեպքերում տվյալների խառը հավաքածուներում անձնական և ոչ անձնական տվյալները չեն կարող անքակտելիորեն փոխկապված լինել՝ տվյալների սուբյեկտին հասանելի դարձնելով միայն տվյալների հավաքածուի անձնական տվյալները: Օրինակ՝ ընկերությանը կարող է անհրաժեշտ լինել տվյալների սուբյեկտին տրամադրել ոչ թե SS խնդիրների վերաբերյալ ընկերության գիտելիքների բազան, այլ առաջացած SS խնդիրների վերաբերյալ առանձին զեկույցներ: Այնուամենայնիվ, հսկողի կողմից ձեռնարկված անվտանգության միջոցները, որպես կանոն, չպետք է ընկալվեն որպես անձնական տվյալներ, եթե դրանք անքակտելիորեն փոխկապված չեն անձնական տվյալների հետ և, հետևաբար, չեն կարգավորվում հասանելիություն ունենալու իրավունքով:

---

[60] Ինչպես վերը նշվել է ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույցում, էջ 10 և վերահաստատվել է ՏՊԵԽ-ի կողմից հաստատված՝ Ավտոմատացված անհատական որոշումների կայացման, այդ թվում՝ պրոֆիլավորման վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույցում, էջ 17:

[61] Անանունացման հասկացության վերաբերյալ լրացուցիչ պարզաբանումներ կարելի է գտնել 29-րդ հոդվածով սահմանված աշխատանքային խմբի Անանունացման տեխնիկաների վերաբերյալ 05/2014 կարծիքում, WP216, 2014 թվականի ապրիլի 10, էջեր 5-19:

[62] Հանձնաժողովի՝ Եվրոպական պառլամենտին և Խորհրդին ուղղված հաղորդագրություն, Եվրոպական միությունում ոչ անձնական տվյալների ազատ հոսքի շրջանակի մասին կանոնակարգի վերաբերյալ ուղեցույց, 2019 թվականի մայիսի 29, COM/2019/250 վերջնական:

101. Մինչև այս բաժինն ամփոփելը, ՏՊԵԽ-ն այս համատեքստում հիշեցնում է, որ անձնական տվյալների մշակման առնչությամբ ֆիզիկական անձանց պաշտպանությունը ներառում է վերը թվարկված անձնական տվյալների բոլոր տեսակները, և որ սահմանման սահմանափակող մեկնաբանությունը հակասում է ՏՊԸԿ դրույթներին և ի վերջո խախտում է Հիմնարար իրավունքների խարտիայի 8-րդ հոդվածը: Անձնական տվյալների որոշ տեսակների նկատմամբ իրավունքի իրացման այլ ռեժիմի կիրառումը, որը նախատեսված չէ ՏՊԸԿ-ով, կարող է ներդրվել բացառապես օրենքով՝ ՏՊԸԿ 23-րդ հոդվածին համապատասխան (ինչպես հաջորդիվ բացատրվում է 6.4 բաժնում): Այսպիսով, հսկողները չեն կարող սահմանափակել հասանելիություն ունենալու իրավունքի իրացումը՝ անհիմն սահմանափակելով անձնական տվյալների շրջանակը:

4.2 Անձնական տվյալները, որոնց վերաբերում է հասանելիություն ունենալու իրավունքը

102. Համաձայն ՏՊԸԿ 15(1) հոդվածի՝ «*տվյալների սուբյեկտն իրավունք ունի հսկողից ստանալու հաստատում այն մասին, թե արդյոք <u>իրեն վերաբերող անձնական տվյալները մշակվում են, թե ոչ</u>, և եթե դրանք մշակվում են, ապա ստանալու անձնական տվյալներին և ստորև նշված տեղեկություններին հասանելիություն*» (շեշտադրումն ավելացված է):

103. Մի քանի տարրեր բխում են ՏՊԸԿ 15-րդ հոդվածի 1-ին կետից: Պարբերությունը հստակորեն [expressis verbis] վերաբերում է «*իրեն վերաբերող անձնական տվյալներին*» (4.2.1), որոնք «*մշակվում են*» (4.2.2) հսկողի կողմից.

4.2.1 «Իրեն վերաբերող անձնական տվյալներ»

104. Հասանելիություն ունենալու իրավունքը կարող է իրացվել բացառապես հասանելիություն ստանալու մասին դիմում ներկայացրած տվյալների սուբյեկտին վերաբերող անձնական տվյալների նկատմամբ կամ, հարկ եղած դեպքում, լիազորված անձի կամ վստահված անձի կողմից (տե՛ս 3.4 բաժինը): Կան նաև իրավիճակներ, երբ տվյալները կապ չունեն հասանելիություն ունենալու իրավունքն իրացնող անձի հետ, այլ կապված են մեկ այլ անձի հետ: Այնուամենայնիվ, տվյալների սուբյեկտն իրավունք ունի ստանալու միայն իրեն վերաբերող անձնական տվյալները՝ բացառությամբ այն տվյալների, որոնք վերաբերում են բացառապես մեկ ուրիշին[63]:

[63] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 9. *«Տվյալների տեղափոխելիության մասին դիմումի շրջանակում ընկնում եմ միայն անձնական տվյալները: Հետևաբար, ցանկացած տվյալ, որն անանուն է կամ չի վերաբերում տվյալների սուբյեկտին, չի ընկնում դրա շրջանակի մեջ: Այնուամենայնիվ, կեղծանունացված տվյալները, որոնք կարող են հստակորեն փոխկապակցվել տվյալների սուբյեկտի հետ (օրինակ՝ նրանց կողմից՝ համապատասխան նույնականացուցիչի տրամադրման միջոցով, տե՛ս 11 (2) հոդվածը), ընկնում են դրա շրջանակի մեջ:*

105. Այնուամենայնիվ, տվյալների դասակարգումը որպես տվյալների սուբյեկտին վերաբերող անձնական տվյալներ, պայմանավորված չէ այն փաստով, որ այդ անձնական տվյալները վերաբերում են նաև մեկ ուրիշին[64]: Այսպիսով, հնարավոր է, որ անձնական տվյալները միաժամանակ վերաբերեն մեկից ավելի անձանց: Սա ինքնաբերաբար չի նշանակում, որ պետք է հասանելիություն ապահովվի այն անձնական տվյալներին, որոնք վերաբերում են նաև մեկ ուրիշին, քանի որ հսկողը պետք է կատարի ՏՊԸԿ 15(4) հոդվածը:

106. «*Իրեն վերաբերող անձնական տվյալներ*» բառերը հսկողների կողմից չպետք է մեկնաբանվեն «*չափազանց սահմանափակող*» ձևով, քանի որ 29-րդ հոդվածով սահմանված աշխատանքային խումբն արդեն հայտարարել է տվյալների տեղափոխելիության իրավունքի մասին[65]: Ինչ վերաբերում է հասանելիություն ունենալու իրավունքին՝ ՏՊԵԽ-ը, օրինակ, համարում է, որ հասանելիություն ստանալու մասին դիմում ներկայացրած տվյալների սուբյեկտի և հսկողի միջև հեռախոսային խոսակցությունների ձայնագրությունները (և դրանց վերծանումը) կարող են կարգավորվել հասանելիություն ունենալու իրավունքով, եթե դրանք անձնական տվյալներ են[66]: Պայմանով, որ կիրառվում է ՏՊԸԿ-ն, և մշակումը չի ընկնում ՏՊԸԿ 2(2)(գ) հոդվածի համաձայն կենցաղային նպատակներով անձնական տվյալների մշակումը բացառելու գործողության ներքո՝ եթե տվյալների սուբյեկտն օգտագործում է ձեռքբերված ձայնագրությունը, որը ներառում է զրուցակցի անձնական տվյալներն այլ նպատակներով, օրինակ՝ հրապարակելով ձայնագրությունը, ապա տվյալների սուբյեկտը կդառնա մեկ այլ անձի անձնական տվյալների այս մշակման համար հսկողը, որի ձայնը ձայնագրվել է: Թեև սա հսկողին չի ազատի տվյալների պաշտպանության իր պարտավորություններից, երբ պատշաճ կերպով վերլուծի, թե արդյոք կարող է հասանելիություն ապահովվել ամբողջական ձայնագրությանը, այնուամենայնիվ, խրախուսվում է, որ հսկողը տեղեկացնի տվյալների սուբյեկտին այն մասին, որ նա կարող է նման դեպքում դառնալ հսկող: Սա չի հակասում ՏՊԸԿ 15(4) հոդվածի համաձայն ցանկացած հետագա գնահատմանը, որը մանրամասնորեն նկարագրված է 6-րդ բաժնում: Նույն կերպ, այն հաղորդագրությունները, որոնք տվյալների սուբյեկտներն ուղարկել են այլ անձանց միջանձնային հաղորդագրությունների տեսքով և ջնջել են իրենց սարքից, որոնք դեռ հասանելի են ծառայություններ մատուցողի համար, կարող են կարգավորվել հասանելիություն ունենալու իրավունքով:

---

[64] ԵՄԱԴ, Պիտեր Նովակն ընդդեմ Տվյալների պաշտպանության հարցերով հանձնակատարի C-434/16 գործով վճիռ, 2017թ., պարբերություն 44:

[65] ՏՊԵԽ-ի կողմից հաստատված՝ Տվյալների տեղափոխելիության իրավունքի վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 9. *Շատ դեպքերում հսկողները կմշակեն այն տեղեկությունները, որոնք պարունակում են մի քանի տվյալների սուբյեկտներին վերաբերող անձնական տվյալներ: Նման դեպքում հսկողները չպետք է չափազանց սահմանափակող մեկնաբանում տան «տվյալների սուբյեկտին վերաբերող անձնական տվյալներ» նախադասությունը: Որպես օրինակ՝ հեռախոսային խոսակցությունները, միջանձնային հաղորդագրությունները կամ VoIP ձայնագրությունները կարող են ներառել (բաժանորդի հաշվի պատմության մեջ) մուտքային և ելքային զանգերի մեջ ներգրավված երրորդ անձանց տվյալները: Թեև ձայնագրությունները, այդպիսով, կպարունակեն բազմաթիվ մարդկանց վերաբերյալ անձնական տվյալներ, այնուամենայնիվ, բաժանորդները պետք կարողանան այդ ձայնագրությունները տրամադրել նրանց՝ ի պատասխան տվյալների տեղափոխելիության մասին դիմումների, քանի որ դրանք (նաև) վերաբերում են տվյալների սուբյեկտին: Այնուամենայնիվ, երբ նման ձայնագրությունները հետագայում փոխանցվում են նոր հսկողին, վերջինս չպետք է դրանք մշակի որևէ նպատակով, որը բացասաբար կանդրադառնա երրորդ անձանց իրավունքների ու ազատությունների վրա (տե՛ս ստորև. երրորդ պայման)»:*

[66] Տե՛ս 6.2 բաժնի 34-րդ օրինակը:

107. Կրկին, կան իրավիճակներ, երբ տվյալների և մի շարք անձանց միջև կապը կարող է հստակ չլինել հսկողի համար, օրինակ՝ անձնական տվյալների գողության դեպքում: Վերջինիս դեպքում անձը խարդախությամբ հանդես է գալիս մեկ այլ անձի անունից: Այս համատեքստում կարևոր է հիշել, որ տուժողին պետք է տեղեկություններ տրամադրել բոլոր այն անձնական տվյալների մասին, որոնք հսկողը պահպանում է նրա ինքնության հետ կապված, այդ թվում՝ այն տվյալները, որոնք հավաքագրվել են խարդախի գործողությունների հիման վրա: Այլ կերպ ասած, նույնիսկ այն բանից հետո, երբ հսկողություն իրականացնող անձը տեղեկացել է անձնական տվյալների գողության մասին, տուժողի ինքնության հետ կապված կամ դրան վերաբերող անձնական տվյալները հանդիսանում են տվյալների սուբյեկտի անձնական տվյալները:

Օրինակ 17. Անձը խաբեությամբ օգտագործում է ուրիշի ինքնությունը՝ առցանց պոկեր խաղալու համար: Հանցագործը վճարում է առցանց խաղատանը՝ օգտագործելով տուժողից գողացված վարկային քարտը: Երբ տուժողը տեղեկանում է անձնական տվյալների գողության մասին, դիմում է առցանց խաղատան կազմակերպչին խնդրանքով իրեն տրամադրել իր անձնական տվյալներին և առավել կոնկրետ՝ հանցագործի խաղացած առցանց խաղերին և վարկային քարտի մասին տեղեկություններին հասանելիություն:

Հավաքված տվյալների և տուժողի միջև առկա է կապ, քանի որ օգտագործվել է վերջինիս ինքնությունը: Խարդախությունը հայտնաբերելուց հետո վերը նշված անձնական տվյալները դեռևս ունեն նրա հետ կապ՝ իրենց բովանդակության (տուժողի վարկային քարտը հստակ վերաբերում է տուժողին), նպատակի և ազդեցության պատճառով (օրինակ՝ հանցագործի խաղացած առցանց խաղերի մասին տեղեկությունները կարող են օգտագործվել՝ տուժողին հաշիվ վավերագրեր ներկայացնելու համար): Հետևաբար, առցանց խաղատունը տուժողին տրամադրում է վերոհիշյալ անձնական տվյալներին հասանելիություն:

108. Անհրաժեշտության դեպքում կարող են օգտագործվել ներքին միացումների մատյաններ՝ ֆայլ մուտք գործելու հետ կապված գրառումները պահելու և վերջինիս հասանելիություն ունենալու առնչությամբ իրականացված այնպիսի գործողություններին հետևելու համար, ինչպիսիք են անձնական տվյալները տպելը, կրկնօրինակելը կամ ջնջելը: Այս մատյանները կարող են ներառել մատյան մուտք գործելու ժամանակը, ֆայլ մուտք գործելու պատճառը, ինչպես նաև մուտք գործած անձին նույնականացնող տեղեկությունները: Այս թեմային առնչվող հարցերը հանդիսանում են ԵՄԱԴ-ում ներկայումս քննվող գործի քննության առարկա (C-579/21): Միացումների մատյանների կիրառումը և վերահսկումն ու գնահատումը գտնվում են հսկողի պատասխանատվության շրջանակներում և ենթակա են ստուգման վերահսկող մարմինների կողմից: Հետևաբար, հսկողը պետք է համոզվի, որ իր իրավասության ներքո գործող անձինք, որոնք հասանելիություն ունեն անձնական տվյալներին, չեն մշակում անձնական տվյալները, քանի դեռ ցուցում չեն ստացել հսկողի կողմից՝ համաձայն ՏՊԸԿ 29-րդ հոդվածի: Այնուամենայնիվ, եթե անձը մշակում է անձնական տվյալները հսկողի ցուցումները կատարելուց բացի այլ նպատակներով, ապա նա կարող է դառնալ այդ մշակման հսկողը և վերջինիս նկատմամբ կարող է հարուցվել կարգապահական կամ քրեական վարույթ կամ վերահսկող մարմինների կողմից կիրառվել վարչական պատասխանատվության միջոց: ՏՊԵԽ-ը նշում է, որ ՏՊԸԿ 24-րդ հոդվածի համաձայն՝ գործատուի պատասխանատվությունն է կիրառել համապատասխան միջոցներ՝ սկսած ուսուցումից մինչև կարգապահական ընթացակարգեր, որպեսզի ապահովի, որ տվյալները մշակվեն ՏՊԸԿ-ին համապատասխան, և որ որևէ խախտում տեղի չունենա:

4.2.2 «Մշակվող» անձնական տվյալները

109. Բացի դրանից, ՏՊԸԿ 15(1) հոդվածը վերաբերում է այն անձնական տվյալներին, որոնք «մշակվում են»: Հասանելիություն ստանալու մասին դիմումի մեջ ներառվող անձնական տվյալների շրջանակը որոշելու ելակետային ժամանակի մասին արդեն ներկայացվել է 2.3.3 բաժնում: Սակայն ձևակերպումը նույնպես հուշում է, որ հասանելիություն ունենալու իրավունքը մշակման գործողությունների նպատակների միջև տարբերակում չի չի մտցնում:

Օրինակ 18. Ընկերությունը մշակել է տվյալների սուբյեկտին վերաբերող անձնական տվյալները՝ նրա գնման պատվերը մշակելու և տվյալների սուբյեկտի տան հասցեով առաքումը կազմակերպելու համար: Այն բանից հետո, երբ այս սկզբնական նպատակները, որոնց համար անձնական տվյալները հավաքվել են, այլևս չկան, հսկողը պահպանում է անձնական տվյալների մի մասը՝ բացառապես հաշվառման հետ կապված իր իրավական պարտավորությունները կատարելու համար:

Տվյալների սուբյեկտը դիմում է իրեն վերաբերող անձնական տվյալներին հասանելիություն տրամադրելու խնդրանքով: ՏՊԸԿ 15(1) հոդվածով նախատեսված իր պարտավորությունը կատարելու համար հսկողը պետք է տվյալների սուբյեկտին տրամադրի պահանջվող անձնական տվյալները, որոնք պահվում են նրա իրավական պարտավորությունները կատարելու համար:

110. Արխիվացված անձնական տվյալները պետք է տարբերվեն պահուստավորված տվյալներից, որոնք բացառապես տվյալների կորստի դեպքում տվյալները վերականգնելու նպատակով պահվող անձնական տվյալներն են: Հարկ է նշել, որ հայեցակարգային տվյալների պաշտպանության սկզբունքների և տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու առումով պահուստային տվյալները սկզբունքորեն նման են ակտիվ համակարգի տվյալներին: Եթե պահուստային և ակտիվ պրոդուկցիոն համակարգում առկա անձնական տվյալների միջև առկա են աննշան տարբերություններ, ապա դրանք հիմնականում կապված են վերջին պահուստավորումից հետո լրացուցիչ տվյալների հավաքագրման հետ: Ակտիվ համակարգում (օրինակ՝ պահպանման ժամկետի ավարտից հետո որոշ տվյալներ ոչնչացնելու պատճառով կամ ոչնչացնելու դիմումից հետո) կրճատված տվյալները որոշ դեպքերում միայն հետագա պահուստավորման ժամանակ կվերագրանցվեն պահուստային տվյալների վրա: Այն դեպքում, երբ ներկայացվել է հասանելիություն ստանալու մասին դիմում այն պահին, երբ պահուստում առկա է տվյալների սուբյեկտին վերաբերող ավելի շատ անձնական տվյալներ, քան ակտիվ համակարգում կամ տարբեր անձնական տվյալներ (նկատելի է, օրինակ՝ տվյալների հավաքագրման ծավալը նվազագույնի հասցնելու սկզբունքին համապատասխան իրականացված՝ ակտիվ պրոդուկցիոն համակարգում առկա ջնջումների մատյանի միջոցով), հսկողը պետք է այս առնչությամբ թափանցիկ լինի, և եթե տեխնիկապես հնարավոր է, ապա ապահովի տվյալների սուբյեկտի կողմից պահանջվող հասանելիությունը, այդ թվում՝ պահուստում պահվող անձնական տվյալներին: Օրինակ՝ իրենց իրավունքներն իրացնող տվյալների սուբյեկտների առջև թափանցիկ լինելու համար ակտիվ պրոդուկցիոն համակարգում ջնջումների մատյանը կարող է հնարավորություն ընձեռել հսկողին տեսնել, որ պահուստում առկա են տվյալներ, որոնք այլևս հասանելի չեն ակտիվ համակարգում, քանի որ դրանք վերջերս ջնջվել են, և դեռևս չեն վերագրանցվել

պահուստում:

4.2.3 Հասանելիություն ստանալու մասին նոր դիմումի շրջանակը

111. Հարկ է նշել, որ տվյալների սուբյեկտներն իրավասու են հասանելիություն ստանալու իրենց վերաբերող բոլոր մշակված տվյալներին կամ տվյալների մի մասին՝ ելնելով դիմումի շրջանակից (տե՛ս նաև տեղեկությունների ամբողջականության վերաբերյալ 2.3.1 բաժինը և դիմումի բովանդակության վերլուծության վերաբերյալ 3.1.1 բաժինը): Համապատասխանաբար, եթե հսկողը նախկինում բավարարել է հասանելիություն ստանալու մասին դիմումը և պայմանով, որ դիմումը սահմանազանցող չէ, հսկողը չի կարող սահմանափակել նոր դիմումի շրջանակը: Սա նշանակում է, որ նույն տվյալների սուբյեկտի հասանելիություն ստանալու մասին ցանկացած հետագա դիմումի առնչությամբ հսկողը չպետք է տեղեկացնի տվյալների սուբյեկտին միայն վերջին դիմումից հետո մշակված անձնական տվյալների կամ բուն մշակման մեջ փոփոխությունների մասին, քանի դեռ տվյալների սուբյեկտը բացահայտ կերպով համաձայնություն չի տվել դրան: Հակառակ դեպքում, տվյալների սուբյեկտները պարտավոր կլինեն հավաքագրել իրենց կողմից տրամադրված անձնական տվյալները՝ մշակման և տվյալների սուբյեկտների իրավունքների վերաբերյալ իրենց տեղեկություններին վերաբերող անձնական տվյալների ամբողջական հավաքածուն ստանալու համար:

4.3 Մշակման և տվյալների սուբյեկտի իրավունքների վերաբերյալ տեղեկությունները

112. Բացի բուն անձնական տվյալների հասանելիությունից, հսկողը պետք է տեղեկություններ տրամադրի մշակման և տվյալների սուբյեկտի իրավունքների մասին՝ համաձայն ՏՊԸԿ 15(1)(ա)-(ը) և 15(2) հոդվածների: Նշված կոնկրետ կետերի վերաբերյալ տեղեկությունների մեծ մասն արդեն հավաքագրված է, առնվազն ընդհանուր ձևով, ՏՊԸԿ 30-րդ հոդվածում և (կամ) ՏՊԸԿ 12-ից 14-րդ հոդվածներին համապատասխան մշակված իր գաղտնիության մասին ծանուցմամբ նշված՝ հսկողի մշակման գործողությունների հաշվառման մատյանում: Հետևաբար, որպես առաջին քայլ կարող է օգտակար լինել ծանոթանալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի «2016/679 կանոնակարգով նախատեսված թափանցիկության վերաբերյալ ուղեցույցին»[67], որը վերաբերում է ՏՊԸԿ 13-րդ և 14-րդ հոդվածների շրջանակներում տրամադրվելիք տեղեկությունների բովանդակությանը:

113. 15(1)(ա)-(ը) հոդվածի և 15(2) հոդվածի կատարման նպատակով հսկողները կարող են զգուշորեն օգտագործել իրենց գաղտնիության մասին ծանուցման տեքստային մոդուլները, եթե նրանք վստահ են, որ դրանք տվյալների սուբյեկտի դիմումի առնչությամբ արդիական են և ճշգրիտ: Տվյալների մշակումից առաջ կամ դրանց մշակման սկզբում որոշ տեղեկություններ, ինչպիսիք են կոնկրետ ստացողների նույնականացումը կամ տվյալների մշակման կոնկրետ տևողությունը, հաճախ դեռևս չեն կարող տրամադրվել:

[67] 29-րդ հոդվածով սահմանված աշխատանքային խումբ, WP260 rev.01, 2018 թվականի ապրիլի 11,

ՏՊԵԽ-ի կողմից հաստատված՝ 2016/679 կանոնակարգի համաձայն թափանցիկության ուղեցույց (այսուհետ՝ ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց):

Որոշ տեղեկություններ, օրինակ՝ վերահսկող մարմին բողոք ներկայացնելու իրավունքը (տե՛ս 15(1)(զ) հոդվածը), չի փոխվում՝ կախված հասանելիություն ստանալու մասին դիմում ներկայացնող անձից: Հետևաբար, դրանք կարող են հաղորդվել ընդհանուր ձևով, քանի որ դրանք ներկայացվում են նաև գաղտնիության մասին ծանուցմամբ: Տեղեկությունների մյուս տեսակները, ինչպիսիք են ստացողների, տվյալների կատեգորիաների և աղբյուրի մասին տեղեկությունները, կարող են տարբվել՝ կախված նրանից, թե ով է ներկայացնում դիմումը, և որն է դիմումի շրջանակը: 15-րդ հոդվածի համաձայն՝ հասանելիություն ստանալու մասին դիմումի համատեքստում մշակման մասին հսկողին հասանելի ցանկացած տեղեկություն պետք է, հետևաբար, թարմացվի և հարմարեցվի դիմում ներկայացնող տվյալների սուբյեկտի առնչությամբ փաստացի իրականացված մշակման գործողություններին: Այսպիսով, իր գաղտնիության քաղաքականության ձևակերպմանը հղում կատարելը բավարար պայման չէ հսկողի համար՝ 15(1)(ա)-(ը) և (2) հոդվածով պահանջվող տեղեկությունները տրամադրելու համար, բացառությամբ, եթե «հարմարեցված և թարմացված» տեղեկությունները նույնն են, ինչ մշակման սկզբում տրամադրված տեղեկությունները: Պարզաբանելով, թե որ տեղեկություններն են վերաբերում դիմում ներկայացնող անձին, հսկողը կարող է, հարկ եղած դեպքում, հղում կատարել որոշ գործողությունների (ինչպես օրինակ՝ «եթե դուք օգտվել եք այս ծառայությունից…», «եթե դուք վճարել եք հաշիվ վավերագրով»), եթե տվյալների սուբյեկտների համար ակնհայտ է, որ դրանք վերաբերում են իրենց: Ստորև պարզաբանվում է տեղեկությունների առանձին տեսակների առնչությամբ պահանջվող հստակեցման աստիճանը:

114. 15(1)(ա) հոդվածի համաձայն՝ նպատակների վերաբերյալ տեղեկությունները պետք է լինեն կոնկրետ՝ դիմում ներկայացնող տվյալների սուբյեկտի կոնկրետ դեպքում կոնկրետ նպատակի (նպատակների) առնչությամբ: Հսկողի ընդհանուր նպատակների թվարկումը բավարար չի լինի, եթե չպարզաբանվի, թե հսկողն ինչ նպատակ (նպատակներ) է հետապնդում դիմում ներկայացնող տվյալների սուբյեկտի կոնկրետ դեպքում: Եթե մշակումն իրականացվում է մի քանի նպատակներով, ապա հսկողը պետք է հստակեցնի, թե որ տվյալները կամ որ կատեգորիայի տվյալներն ինչ նպատակով (նպատակներով) են մշակվում: Ի տարբերություն ՏՊԸԿ 13(1)(գ) հոդվածի և 14(1)(գ) հոդվածի՝ 15(1)(ա) հոդվածում նշված մշակման մասին տեղեկությունները չեն պարունակում մշակման իրավական հիմքերի մասին տեղեկություններ: Այնուամենայնիվ, քանի որ տվյալների սուբյեկտների որոշ իրավունքներ կախված են կիրառելի իրավական հիմքից, այս տեղեկությունները կարևոր են տվյալների սուբյեկտների համար՝ ստուգելու տվյալների մշակման օրինականությունը և որոշելու, թե տվյալների սուբյեկտի որ իրավունքներն են կիրառելի կոնկրետ իրավիճակում: Հետևաբար, ՏՊԸԿ 12(2) հոդվածի համաձայն տվյալների սուբյեկտների իրավունքների իրացումը դյուրացնելու համար ցանկալի է, որ հսկողը տեղեկացնի նաև տվյալների սուբյեկտին յուրաքանչյուր մշակման գործողության համար կիրառելի իրավական հիմքի մասին կամ նշի, թե որտեղ նրանք կարող են գտնել այդ տեղեկությունները: Ամեն դեպքում, թափանցիկ մշակման սկզբունքը պահանջում է, որ մշակման իրավական հիմքերի վերաբերյալ տեղեկությունները հասանելի լինեն տվյալների սուբյեկտին մատչելի ձևով (օրինակ՝ գաղտնիության մասին ծանուցմամբ):

115. Տվյալների կատեգորիաների վերաբերյալ տեղեկությունները (15(1)(բ) հոդված) նույնպես կարող են հարմարեցվել տվյալների սուբյեկտի իրավիճակին այնպես, որ դիմողի դեպքում կարևորություն չներկայացնող տվյալների կատեգորիաները վերացվեն:

Օրինակ 19. ՏՊԸԿ 13/14 հոդվածներում նշված տեղեկությունների համատեքստում հյուրանոցը նշում է, որ իրենք մշակում են հաճախորդների մի շարք կատեգորիաների տվյալներ (նույնականացման տվյալներ, կոնտակտային տվյալներ, բանկային տվյալներ և վարկային քարտի համար և այլն): Եթե հասանելիություն ստանալու մասին դիմումը ներկայացվում է 15-րդ հոդվածի հիման վրա, ապա դիմում ներկայացնող տվյալների սուբյեկտը, մշակվող փաստացի տվյալներին հասանելիություն ստանալուց բացի (բաղադրիչ 2), պետք է, 15(1)(բ) հոդվածին համապատասխան, տեղեկացված լինի նաև կոնկրետ դեպքում մշակվող հատուկ կատեգորիայի տվյալների մասին (օրինակ՝ չներառելով բանկային տվյալները կամ վարկային քարտի տվյալները, եթե վճարումը կատարվել է կանխիկ):

116. «Ստացողների կամ ստացողների կատեգորիաների» մասին տեղեկություններով (15(1)(գ) հոդված) նախևառաջ պետք է հաշվի առնվի ՏՊԸԿ 4(9) հոդվածում տրված ստացողների սահմանումը: Ստացողների սահմանումը հիմնված է անձնական տվյալների՝ ֆիզիկական կամ իրավաբանական անձին, պետական մարմնին, գերատեսչությանը կամ այլ մարմնին հրապարակման վրա[68]: ՏՊԸԿ 4(9) հոդվածից հետևում է, որ պետական մարմինները, որոնք գործում են կոնկրետ հարցման շրջանակներում, հատուկ ազգային դրույթների հաշվառմամբ, չպետք է համարվեն ստացողներ:

117. Ինչ վերաբերում է այն հարցին, թե արդյոք հսկողն ազատ է ընտրություն կատարել ստացողների կամ ստացողների կատեգորիաների վերաբերյալ տեղեկությունների միջև՝ հարկ է նշել, որ «ի տարբերություն ՏՊԸԿ 13-րդ և 14-րդ հոդվածների, որոնք հսկողի համար պարտավորություն են սահմանում (…), ՏՊԸԿ 15-րդ հոդվածը սահմանում է տվյալների սուբյեկտի համար հասանելիություն ունենալու իրական իրավունք, որի արդյունքում տվյալների սուբյեկտը պետք է հնարավորություն ունենա կա՛մ տեղեկություններ ստանալու կոնկրետ ստացողների մասին, թե տվյալները ում են տրամադրվել կամ ում կհրապարակվեն, եթե դա հնարավոր է, կա՛մ տեղեկություններ ստանալու ստացողների կատեգորիաների մասին»:[69] Հարկ է նաև հիշել, որ, ինչպես նշված է թափանցիկության վերաբերյալ վերը նշված ուղեցույցում[70], արդեն ՏՊԸԿ 13-րդ և 14-րդ հոդվածների համաձայն ստացողներին կամ ստացողների կատեգորիաներին վերաբերող տեղեկությունները պետք է հնարավորինս կոնկրետ լինեն՝ թափանցիկության և արդարության սկզբունքների առումով: 15-րդ հոդվածի համաձայն, եթե տվյալների սուբյեկտն այլ բան չի ընտրել, ապա հսկողը պարտավոր է նշել փաստացի ստացողների անունները, բացառությամբ այն դեպքերի, երբ անհնար է նույնականացնել այդ ստացողներին, կամ հսկողն ապացուցում է, որ տվյալների սուբյեկտի՝ հասանելիություն ստանալու մասին դիմումներն ակնհայտորեն անհիմն են կամ սահմանազանցող՝ ՏՊԸԿ 12(5) հոդվածի իմաստով[71][72]: ՏՊԵԽ-ն այս կապակցությամբ հիշեցնում է, որ փաստացի ստացողներին վերաբերող տեղեկությունների պահպանումն անհրաժեշտ է, որպեսզի *ի թիվս այլնի*, հնարավոր լինի կատարել հսկողի՝ ՏՊԸԿ 5(2) և 19-րդ հոդվածների համաձայն ստանձնած պարտավորությունները:

[68] Հարկ է նաև նշել, որ նույն ընկերությունում կարող են լինել ՏՊԸԿ 4(7) հոդվածով սահմանված հսկողներ: Այս աստղաբույլում հնարավոր է մեկ ընկերության ներսում տվյալների հրապարակում մեկ ստացողից մյուսին:

Օրինակ 20. Գործատուն իր գաղտնիության մասին ծանուցման մեջ տեղեկություններ է տրամադրում այն մասին, թե ինչ կատեգորիաների տվյալներ են գործուղումների դեպքում փոխանցվում «տուրիստական գործակալություններին» կամ «հյուրանոցներին»՝ ՏՊԸԿ 13(1)(ե) և 14(1)(ե) հոդվածների համաձայն: Եթե աշխատողը գործուղումներից հետո ներկայացնում է անձնական տվյալներին հասանելիություն ստանալու մասին դիմում, ապա գործատուն պետք է, 15(1)(գ) հոդվածի համաձայն, անձնական տվյալներ ստացողների վերաբերյալ նշի այն տուրիստական գործակալությանը (գործակալություններին) և հյուրանոցին (հյուրանոցներին), որոնք ստացել են տվյալները: Թեև գործատուն իր գաղտնիության մասին ծանուցման մեջ իրավաչափ կերպով նշել է ստացողների կատեգորիաները՝ 13-րդ և 14-րդ հոդվածների համաձայն, քանի որ այս փուլում դեռևս հնարավոր չի եղել նշել ստացողների անունները, նա պետք է, աշխատողի կողմից այլ բան չընտրելու դեպքում, տրամադրի կոնկրետ ստացողներին վերաբերող տեղեկություններ (տուրիստական գործակալությունների, հյուրանոցների անվանումը և այլն), երբ աշխատողը ներկայացնում է հասանելիություն ստանալու մասին դիմում:

Եթե վերը նշված պայմանների պահպանմամբ հսկողը կարող է տրամադրել միայն ստացողների կատեգորիաները, ապա տեղեկությունները պետք է լինեն հնարավորինս կոնկրետ՝ նշելով ստացողի տեսակը (այսինքն՝ հղում կատարելով այն գործողություններին, որոնք նա իրականացնում է), բնագավառը, ոլորտն ու ենթաոլորտը և ստացողների գտնվելու վայրը[73]:

118. 15(1)(դ) հոդվածի համաձայն՝ հնարավորության դեպքում տեղեկությունները պետք է տրամադրվեն նախատեսված այն ժամանակահատվածի համար, որի ընթացքում պահպանվելու են անձնական տվյալները: Հակառակ դեպքում, պետք է ներկայացվեն այդ ժամանակահատվածը որոշելու համար կիրառվող չափանիշները: Հսկողի կողմից տրված տեղեկությունները պետք է բավականաչափ ճշգրիտ լինեն, որպեսզի տվյալների սուբյեկտն իմանա, թե որքան ժամանակ են իրեն վերաբերող տվյալները պահպանվելու: Եթե հնարավոր չէ նշել ջնջելու ժամանակը, ապա պետք է նշվեն պահպանման ժամկետները և այդ ժամանակահատվածի սկիզբը կամ դրդող իրադարձությունը (օրինակ՝ պայմանագրի գործողության դադարեցումը, երաշխիքային ժամկետի ավարտը և այլն): Օրինակ՝ «օրենքով սահմանված պահպանման ժամկետները լրանալուց հետո ջնջելուն» պարզապես հղում կատարելը բավարար չէ: Տվյալների պահպանման ժամկետների վերաբերյալ նշումներում պետք է շեշտը դրվի տվյալների սուբյեկտին վերաբերող կոնկրետ տվյալների վրա: Եթե տվյալների սուբյեկտի անձնական տվյալները ենթակա են ջնջման տարբեր ժամկետներում (քանի որ ոչ բոլոր տվյալների վրա են տարածվում պահպանման իրավական պարտավորությունները), ապա համապատասխան մշակման գործողությունների և տվյալների կատեգորիաների առնչությամբ նշվում են ջնջման ժամկետները:

---

[69] ԵՄԱԴ, գործ թիվ C-154/21 (Österreichische Post AG), պարբերություն 36:

[70] 29-րդ հոդվածով սահմանված աշխատանքային խումբ, WP260 rev.01, 2018 թվականի ապրիլի 11, ՏՊԵԽ-ի կողմից հաստատված՝ 2016/679 կանոնակարգի համաձայն թափանցիկության ուղեցույց (այսուհետ՝ ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց), էջ 37 (հավելված):

[71] ԵՄԱԴ, գործ թիվ C-154/21 (Österreichische Post AG):

[72] Պարզապես այն փաստը, որ տվյալները հրապարակվել են մեծ թվով ստացողների, ինքնին չի դարձնի դիմումը սահմանազանցող, տե՛ս 6-րդ բաժինը, պարբերություն 188:

[73] ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, էջ 37 (հավելված)

119. Թեև վերահսկող մարմին բողոք ներկայացնելու իրավունքի մասին տեղեկությունները (15(1)(զ) հոդված) կախված չեն կոնկրետ հանգամանքներից, այնուամենայնիվ, 15(1)(ե) հոդվածում նշված տվյալների սուբյեկտների իրավունքները տարբերվում են՝ կախված մշակման հիմքում ընկած իրավական հիմքից: Ինչ վերաբերում է ՏՊԸԿ 12(2) հոդվածի համաձայն տվյալների սուբյեկտի իրավունքների իրացումը դյուրացնելու իր պարտավորությանը՝ այդ իրավունքների վերաբերյալ հսկողի պատասխանն անհատապես հարմարեցվում է տվյալների սուբյեկտի դեպքին և վերաբերում է համապատասխան մշակման գործողություններին: Անհրաժեշտ է խուսափել կոնկրետ իրավիճակում տվյալների սուբյեկտի նկատմամբ չկիրառվող իրավունքների մասին տեղեկություններից:

120. 15(1)(է) հոդվածի համաձայն՝ տվյալների աղբյուրի վերաբերյալ «ցանկացած հասանելի տեղեկություն» պետք է տրամադրվի, եթե անձնական տվյալները չեն հավաքագրվել տվյալների սուբյեկտից: Հասանելի տեղեկությունների աստիճանը կարող է փոփոխվել ժամանակի ընթացքում:

Օրինակ 21. Խոշոր ընկերության գաղտնիության քաղաքականությամբ նշվում է.

«Վարկունակության ստուգումն օգնում է մեզ կանխել վճարային գործարքների հետ կապված խնդիրները: Դրանք երաշխավորում են մեր ընկերության պաշտպանությունը ֆինանսական ռիսկերից, որոնք միջնաժամկետ և երկարաժամկետ հեռանկարում կարող են ազդել նաև վաճառքի գների վրա: Վարկունակության ստուգումը պարտադիր կերպով իրականացվում է, երբ մենք պատրաստվում ենք առաքել ապրանքներ՝ միաժամանակ չստանալով համապատասխան գնման գինը, օրինակ՝ ապառիկ գնման դեպքում: Առանց վարկունակության ստուգման հնարավոր է միայն կանխավճարի վճարման տարբերակը (արագ բանկային փոխանցում, առցանց վճարման ծառայություններ մատուցողներ, կրեդիտ քարտ):

Վարկունակության ստուգման նպատակով մենք Ձեր անունը, հասցեն և ծննդյան ամսաթիվը կուղարկենք հետևյալ ծառայություններ մատուցողներին, օրինակ՝ 1) X ֆինանսական տեղեկությունների հարցերով գործակալությանը, 2) Y գործարար տեղեկությունների մատակարարին, 3) Z վարկային բյուրոյին:

Տվյալները փոխանցվում են վերոնշյալ վարկային կազմակերպություններին միայն այն ծավալով, որքանով թույլատրվում է օրենքով և միայն Ձեր նախկին վճարումների վարքագծի վերլուծության, հասցեի տվյալներն օգտագործելով մաթեմատիկավիճակագրական ընթացակարգերի հիման վրա անվճարունակության ռիսկի գնահատման, ինչպես նաև Ձեր հասցեի ստուգման նպատակներով (առաքման ուսումնասիրություն): Կախված վարկունակության ստուգման արդյունքից՝ մենք այլևս չենք կարողանա Ձեզ առաջարկել վճարման անհատական մեթոդներ, ինչպես օրինակ՝ հաշիվ վավերագրերի գնումը»:

Այսպիսով, գաղտնիության մասին ծանուցումը պարունակում է ընդհանուր տեղեկություններ նշված Տնտեսական տեղեկությունների հարցերով գրասենյակներից տեղեկություններ ստանալու հնարավորության մասին՝ ՏՊԸԿ 13-րդ և 14-րդ հոդվածներին համապատասխան: Եթե նախնական ուսումնասիրությունից պարզ չի դառնում, թե որ ընկերություններն են ներգրավելու մշակման գործընթացին, ապա բավարար է գաղտնիության քաղաքականության մեջ նշել իրավասու ընկերությունների անվանումները: 15-րդ հոդվածի հիման վրա ներկայացված դիմումի համատեքստում, ի լրումն այն տեղեկությունների, որ վարկունակության վերաբերյալ տեղեկությունները ձեռք են բերվել, այնուհետև (հետագայում) անհրաժեշտ կլինի հրապարակել, թե նշված ընկերություններից կոնկրետ որ ընկերություններն են ներգրավել գործընթացին: 15(1)(է) հոդվածում հստակ նշված է, որ տվյալների մշակման վերաբերյալ տեղեկությունները ներառում են «դրանց աղբյուրի վերաբերյալ ցանկացած տեղեկություն», եթե անձնական տվյալները չեն հավաքվում տվյալների սուբյեկտից:

121. 15(1)(ը) հոդվածով նախատեսվում է, որ յուրաքանչյուր տվյալների սուբյեկտ պետք է իրավունք ունենա արժանահավատ կերպով տեղեկացված լինելու, ի թիվս այլնի, ավտոմատացված որոշումների կայացման գոյության և դրանց հիմքում ընկած տրամաբանության մասին, այդ թվում՝ տվյալների սուբյեկտի պրոֆիլավորման, ինչպես նաև այդ մշակման կարևորության և հնարավոր հետևանքների մասին[74]: Հնարավորության դեպքում 15(1)(ը) հոդվածով նախատեսված տեղեկությունները պետք է առավել կոնկրետ լինեն այն փաստարկի առնչությամբ, որը հանգեցնում է հասանելիություն հայցած տվյալների սուբյեկտին վերաբերող հատուկ որոշումների կայացմանը:

122. Երրորդ երկիր կամ միջազգային կազմակերպություն տվյալների ակնկալվող փոխանցումների վերաբերյալ տեղեկությունները, այդ թվում՝ միջոցների բավարար լինելու մասին Հանձնաժողովի որոշման կամ համապատասխան երաշխիքների առկայությունը պետք է նախատեսվեն՝ ՏՊԸԿ 13(1)(զ) և 14(1)(զ) հոդվածների համաձայն: 15-րդ հոդվածով նախատեսված հասանելիություն ստանալու մասին դիմումի համատեքստում 15(2) հոդվածներով պահանջվում են համապատասխան երաշխիքների վերաբերյալ տեղեկություններ՝ ՏՊԸԿ 46-րդ հոդվածի համաձայն միայն այն դեպքերում, երբ իրականում տեղի ունենում է տվյալների փոխանցում երրորդ երկիր կամ միջազգային կազմակերպություն:

5 ԻՆՉՊԵ՞Ս ԿԱՐՈՂ Է ՀՍԿՈՂՆ ԱՊԱՀՈՎԵԼ ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ

123. ՏՊԸԿ-ն շատ նորմատիվ բնույթ չի կրում հսկողի կողմից հասանելիություն ապահովելու եղանակի առումով: Հասանելիություն ունենալու իրավունքը կարող է որոշ իրավիճակներում լինել հեշտ և պարզ կիրառելի, օրինակ, երբ փոքր կազմակերպությունը տվյալների սուբյեկտի վերաբերյալ տիրապետում է սահմանափակ տեղեկությունների: Այլ իրավիճակներում հասանելիություն ունենալու իրավունքն ավելի բարդ է, քանի որ տվյալների մշակումն ավելի բարդ է՝ կապված տվյալների սուբյեկտների թվի, մշակվող տվյալների կատեգորիաների, ինչպես նաև տարբեր կազմակերպություններում և դրանցից դուրս տվյալների հոսքի հետ: Հաշվի առնելով անձնական տվյալների մշակման տարբերությունները՝ հասանելիության ապահովման պատշաճ եղանակը կարող է համապատասխանաբար տարբերվել:

124. Սույն բաժնի նպատակը հսկողների՝ հասանելիություն ստանալու մասին դիմումները բավարարելու տարբեր եղանակների, ինչպես նաև հասանելիություն ունենալու իրավունքի առնչությամբ ՏՊԸԿ 12(1) հոդվածի իմաստի վերաբերյալ որոշ ուղղորդումներ և գործնական օրինակներ տրամադրելն է: Սույն բաժնով կտրամադրվեն նաև որոշ ուղղորդումներ այն մասին, թե ինչն է սովորաբար համարվում լայնորեն կիրառվող էլեկտրոնային եղանակ, ինչպես նաև ՏՊԸԿ 12(3) հոդվածով նախատեսված հասանելիություն ապահովելու ժամկետների մասին:

[74] Տե՛ս 2016/679 կանոնակարգի համաձայն թափանցիկության ուղեցույցը (WP 260), պարբերություն 41՝ հղում կատարելով 2016/679 կանոնակարգի նպատակներով ավտոմատացված անհատական որոշումների կայացման, այդ թվում՝ պրոֆիլավորման վերաբերյալ ուղեցույցին (WP 251):

5.1 Ինչպե՞ս կարող է հսկողն առբերել պահանջվող տվյալները

125. Տվյալների սուբյեկտները պետք է հասանելիություն ունենան իրենց վերաբերող այն բոլոր տեղեկություններին, որոնք հսկողը մշակում է: Սա նշանակում է, օրինակ, որ հսկողը պարտավոր է անձնական տվյալները որոնել իր SS համակարգերում և SS-ի հետ առնչություն չունեցող հաշվառման համակարգերում: Տվյալները որոնելիս հսկողը պետք է օգտագործի տվյալների սուբյեկտի վերաբերյալ կազմակերպությունում առկա տեղեկությունները, որոնք ամենայն հավանականությամբ կհամընկնեն համակարգերում՝ ելնելով այն հանգամանքից, թե տեղեկություններն ինչպես են համակարգված[75]: Օրինակ, եթե տեղեկությունները սորտավորված են ֆայլերում անուններով կամ հղման համարներով, ապա որոնումը կարող է սահմանափակվել այս գործոններով: Սակայն եթե տվյալների կառուցվածքը կախված է այլ գործոններից, ինչպես օրինակ՝ ընտանեկան հարաբերություններից կամ մասնագիտական կոչումներից կամ ցանկացած տեսակի ուղղակի կամ անուղղակի նույնականացուցիչներից (օրինակ՝ հաճախորդի համարը, օգտատիրոջ անունը կամ IP հասցեները), ապա որոնումը պետք է ընդլայնել՝ դրանք ներառելով որոնման մեջ՝ պայմանով, որ հսկողը տիրապետում է նաև տվյալների սուբյեկտին վերաբերող այս տեղեկությունները, կամ այդ տեղեկությունները տրամադրվում են տվյալների սուբյեկտի կողմից: Նույնը վերաբերում է այն դեպքերին, երբ երրորդ անձանց վերաբերող տվյալները կարող են պարունակել տվյալների սուբյեկտին վերաբերող անձնական տվյալներ: Այնուամենայնիվ հսկողը կարող է չպահանջել տվյալների սուբյեկտից տրամադրել ավելի շատ տեղեկություններ, քան անհրաժեշտ է՝ տվյալների սուբյեկտին նույնականացնելու համար: Եթե հսկողն իր տվյալների մշակման գործողությունների մեջ ներգրավում է մշակողին, ապա որոնումը բնականաբար պետք է ընդլայնվի՝ ներառելու համար նաև մշակողի կողմից մշակված անձնական տվյալները:

126. ՏՊԸԿ տվյաների՝ հայեցակարգային և լռելյայն պաշտպանության մասին 25-րդ հոդվածի համաձայն՝ հսկողը (և մշակման գործընթացին նրա կողմից ներգրավված ցանկացած մշակող) նույնպես պետք է արդեն իրականացրած լիներ այն գործառույթները, որոնք հնարավորություն կտային պահպանել տվյալների սուբյեկտի իրավունքները: Այս համատեքստում սա նշանակում է, որ դիմումին ընթացք տալու ժամանակ տվյալների սուբյեկտի վերաբերյալ տեղեկություններ գտնելու և առբերելու համար պետք է առկա լինեն համապատասխան մեխանիզմներ: Այնուամենայնիվ, հարկ է նշել, որ այս առումով սահմանազանցող մեկնաբանությունը կարող է հանգեցնել տեղեկությունների որոնման և առբերման գործառույթների, որոնք ինքնին վտանգ են ներկայացնում տվյալների սուբյեկտների անձեռնմխելիության համար: Հետևաբար, կարևոր է նկատի ունենալ, որ տվյալների առբերման գործընթացը պետք է նույնպես իրականացվի տվյալների պաշտպանության պահանջների հաշվառմամբ, որպեսզի այն չվտանգի այլ անձանց, օրինակ՝ հսկողի աշխատողների անձեռնմխելիությունը:

[75] Այդ որոնումն անշուշտ պետք է ներառի նաև այն տեղեկությունները, որոնց տիրապետում է մշակողը, տե՛ս ՏՊԸԿ 28(3)(ե) հոդված

5.2 Հասանելիություն ապահովելու համար համապատասխան միջոցները

5.2.1 «Համապատասխան միջոցներ» ձեռնարկելը

127. ՏՊԸԿ 12-րդ հոդվածով սահմանվում են հասանելիություն ապահովելու պահանջները, այսինքն՝ 15-րդ հոդվածի համաձայն՝ հաստատումը, անձնական տվյալները և լրացուցիչ տեղեկություններ տրամադրելու պահանջները, ինչպես նաև հասանելիություն ունենալու իրավունքի ձևը, եղանակը և ժամկետը: 2016/679 կանոնակարգի համաձայն թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույցը[76] լրացուցիչ ուղղորդում է տրամադրում ՏՊԸԿ 12-րդ հոդվածի, մասնավորապես 13-րդ և 14-րդ հոդվածների, ինչպես նաև 15-րդ հոդվածի և ընդհանրապես թափանցիկության առնչությամբ: Այսպիսով, այդ ուղեցույցում սահմանվածները կարող են հաճախ հավասարապես կիրառվել 15-րդ հոդվածով նախատեսված հասանելիություն ապահովելու նկատմամբ:

128. ՏՊԸԿ 12(1) հոդվածով սահմանվում է, որ հսկողը ձեռնարկում է պատշաճ միջոցներ, որպեսզի տվյալների սուբյեկտին հակիրճ, թափանցիկ, հասկանալի և հեշտ հասանելի ձևով, պարզ ու հասարակ լեզվով տրամադրի մշակման հետ կապված ցանկացած հաղորդակցություն՝ 15-րդ հոդվածին համապատասխան: 12(2) հոդվածով սահմանվում է, որ հսկողը դյուրացնում է տվյալների սուբյեկտի հասանելիություն ունենալու իրավունքի իրացումը: Այս առումով ավելի հստակ պահանջները պետք է գնահատվեն յուրաքանչյուր կոնկրետ դեպքում: Պատշաճ միջոցներ կիրառելու վերաբերյալ որոշում կայացնելիս հսկողները պետք է հաշվի առնեն բոլոր համապատասխան հանգամանքները, այդ թվում՝ մշակվող տվյալների քանակը, դրանց մշակման բարդությունը և իրենց տվյալների սուբյեկտների մասին ունեցած տեղեկությունները, օրինակ, եթե տվյալների սուբյեկտների մեծ մասը երեխաներ են, տարեցներ կամ հաշմանդամություն ունեցող անձինք, սակայն չպետք է սահմանափակվեն դրանցով: Բացի դրանից, այն իրավիճակներում, երբ հսկողը տեղեկացվում է դիմում ներկայացրած տվյալների սուբյեկտի որևէ կոնկրետ կարիքի մասին, օրինակ՝ ներկայացված դիմումի մեջ առկա լրացուցիչ տեղեկությունների միջոցով, նա պետք է հաշվի առնի այդ հանգամանքները: Արդյունքում կիրառվող պատշաճ միջոցները կտարբերվեն:

129. Գնահատում կատարելիս կարևոր է նկատի ունենալ, որ «պատշաճ» եզրույթը երբեք չպետք է ընկալվի որպես հասանելիություն ունենալու իրավունքով կարգավորվող տվյալների շրջանակը սահմանափակող միջոց: «Պատշաճ» եզրույթը չի նշանակում, որ տեղեկություններ տրամադրելու ջանքերը կարող են հակակշռվել, օրինակ՝ ցանկացած այն շահի հետ, որը կարող է ունենալ տվյալների սուբյեկտը՝ անձնական տվյալներ ստանալու հարցում: Փոխարենը, գնահատումը պետք է նպատակաուղղված լինի այս իրավունքով կարգավորվող բոլոր տեղեկությունների տրամադրման ամենահարմար մեթոդի ընտրությանը՝ ելնելով յուրաքանչյուր դեպքի կոնկրետ հանգամանքներից: Արդյունքում, հսկողը, որը մշակում է մեծ մասշտաբով, մեծ քանակությամբ տվյալներ, պետք է գործադրի մեծ ջանքեր, որպեսզի տվյալների սուբյեկտներին հակիրճ, թափանցիկ, հասկանալի և հեշտ հասանելի ձևով, հասարակ ու պարզ լեզվով տրամադրի հասանելիություն ունենալու իրավունք:

[76] 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, WP260 rev.01, 2018 թվականի ապրիլի 11, ՏՊԵՒ-ի կողմից հաստատված՝ 2016/679 կանոնակարգի համաձայն թափանցիկության ուղեցույց (այսուհետ՝ ՏՊԵՒ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց):

130. Անհրաժեշտ է խուսափել տվյալներին հասանելիություն ստանալու մասին դիմումին ի պատասխան տվյալների սուբյեկտին տարբեր աղբյուրներ ուղղորդելուց: Ինչպես նշվել է Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույցում (ՏՊԸԿ 13-րդ և 14-րդ հոդվածներում «տրամադրել» հասկացության հետ կապված), *«տրամադրել»* հասկացությունը ենթադրում է, որ *«տվյալների սուբյեկտը չպետք է ակտիվորեն փնտրի այդ հոդվածներով նախատեսված տեղեկությունները, ի թիվս այլ տեղեկությունների, ինչպես օրինակ՝ կայքի կամ հավելվածի օգտագործման պայմանները»*[77]: Հետևաբար, թափանցիկության սկզբունքին համապատասխան, տվյալների սուբյեկտները պետք է հսկողից ձեռք բերեն 15(1), 15(2) և 15(3) հոդվածներով պահանջվող տեղեկություններն ու անձնական տվյալներն այնպես, որը կարողանան ստանալ տեղեկությունների ամբողջական հասանելիություն: Հատուկ դեպքերում, օրինակ՝ տեղեկությունների (ազդարարման հետ կապված տեղեկությունների) գաղտնիության պատճառով հսկողին տեղեկություններ տրամադրելը տեղին չի լինի կամ նույնիսկ կհամարվի անօրինական: Այս դեպքերում տեղին կհամարվի տվյալների սուբյեկտների հասանելիություն ստանալու մասին դիմումին ի պատասխան տեղեկությունները բաժանել մի քանի պատասխանների: Հսկողի կողմից ընտրված մեթոդով պետք է տվյալների սուբյեկտին փաստացի տրամադրվի պահանջվող տվյալներն ու տեղեկությունները, հետևաբար տեղին չի լինի տվյալների սուբյեկտին միայն ուղղորդել, որպեսզի վերջինս ստուգի պահանջվող տվյալները, որոնք պահվում են իր սարքում, այդ թվում, օրինակ՝ իր բջջային հեռախոսով կայքէջեր կատարած այցելությունների պատմությունը և IP հասցեները:

131. Հաշվետվողականության սկզբունքին համապատասխան՝ հսկողը պետք է փաստաթղթավորի իր մոտեցումը, որպեսզի կարողանա ապացուցել, թե ինչպես են 15-րդ հոդվածով նախատեսված տեղեկությունները տրամադրելու համար ընտրված միջոցները տվյալ դեպքում համարվում պաշտաճ:

5.2.2 Հասանելիություն ապահովելու տարբեր միջոցները

132. Ինչպես արդեն ներկայացվել է վերևում՝ 2.2.2 բաժնում, հասանելիություն ստանալու մասին դիմում ներկայացնելիս տվյալների սուբյեկտներն իրավունք ունեն ստանալու 15(3) հոդվածի համաձայն մշակվող իրենց տվյալների կրկնօրինակը, ինչպես նաև լրացուցիչ տեղեկություններ, ինչը համարվում է անձնական տվյալներին հասանելիություն ապահովելու հիմնական մեթոդը:

---

[77] ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, պարբերություն 33:

133. Այնուամենայնիվ, որոշ դեպքերում հսկողի համար կարող է նպատակահարմար լինել հասանելիություն ապահովել կրկնօրինակը տրամադրելուց բացի այլ եղանակներով: Հասանելիության այդ ոչ մշտական մեթոդները կարող են լինել, օրինակ՝ բանավոր տեղեկությունները, ֆայլերի ստուգումը, տեղում կամ հեռավար հասանելիությունը՝ առանց ներբեռնման հնարավորության: Այս մեթոդները կարող են հասանելիություն ապահովելու համար պատշաճ եղանակներ լինել, օրինակ՝ այն դեպքերում, երբ դա բխում է տվյալների սուբյեկտի շահերից, կամ երբ տվյալների սուբյեկտն է դա պահանջում: Տեղում հասանելիությունը նույնպես կարող է նպատակահարմար լինել, որպես նախնական միջոց, երբ հսկողը մշակում է մեծ քանակությամբ չթվայնացված տվյալներ, որպեսզի տվյալների սուբյեկտը տեղեկացված լինի, թե ինչ անձնական տվյալներ են մշակվում և կարողանա տեղեկացված որոշում կայացնել այն մասին, թե ինչ անձնական տվյալներ է նա ցանկանում ստանալ կրկնօրինակի միջոցով: Հասանելիության ոչ մշտական ուղիները որոշակի իրավիճակներում կարող են բավարար և համարժեք լինել, օրինակ՝ այն կարող է բավարարել տվյալների սուբյեկտների կարիքը՝ ստուգելու, որ հսկողի կողմից մշակված տվյալները ճիշտ են՝ տվյալների սուբյեկտներին հնարավորություն տալով ծանոթանալ սկզբնական տվյալներին: Հսկողը պարտավոր չէ կրկնօրինակը տրամադրելուց բացի տեղեկություններ տրամադրել այլ եղանակներով, սակայն այդ դիմումը քննարկելիս պետք է կիրառի ողջամիտ մոտեցում: Կրկնօրինակները տրամադրելուց բացի այլ եղանակներով հասանելիություն ապահովելը տվյալների սուբյեկտներին չի զրկում նաև կրկնօրինակն ունենալու իրավունքից, եթե նրանք որոշում են ձեռք բերել այն:

134. Կախված իրավիճակից՝ հսկողը կարող է ընտրել մշակվող տվյալների կրկնօրինակը, ինչպես նաև լրացուցիչ տեղեկությունները տրամադրել տարբեր եղանակներով, օրինակ՝ էլ. փոստի, սովորական փոստի կամ ինքնասպասարկման գործիքի կիրառման միջոցով: Եթե տվյալների սուբյեկտը դիմումը ներկայացնում է էլեկտրոնային միջոցներով, և եթե տվյալների սուբյեկտն այլ բան չի պահանջում, ապա տեղեկությունները տրամադրվում են 15(3) հոդվածում նշված՝ լայնորեն կիրառվող էլեկտրոնային եղանակով: Ամեն դեպքում հսկողը պետք է դիտարկի նպատակահարմար տեխնիկական և կազմակերպչական միջոցներ, այդ թվում՝ տեղեկություններն էլ. փոստի կամ առցանց ինքնասպասարկման գործիքների միջոցով տրամադրելիս համարժեք գաղտնագրում կիրառելու հնարավորությունը:

135. Այն դեպքում, երբ հսկողը միայն փոքր մասշտաբով է մշակում դիմում ներկայացնող անձին վերաբերող անձնական տվյալները, անձնական տվյալների և լրացուցիչ տեղեկությունների կրկնօրինակը կարող է և պետք է տրամադրվի պարզ ընթացակարգով:

Օրինակ 22. Տեղական գրախանութը վարում է տուն առաքում պատվիրած իրենց հաճախորդների անունների և հասցեների հաշվառում: Հաճախորդն այցելում է գրախանութ և տվյալներին հասանելիություն ստանալու մասին դիմում է ներկայացնում: Այս իրավիճակում բավական է անմիջապես բիզնես համակարգից տպել հաճախորդին վերաբերող անձնական տվյալները՝ միաժամանակ նաև տրամադրելով 15(1) և (2) հոդվածով նախատեսված լրացուցիչ տեղեկությունները:

Օրինակ 23. Բարեգործական կազմակերպության ամեն ամիս նվիրատվություն կատարող անձը տվյալներին հասանելիություն ստանալու մասին դիմում է ներկայացնում էլ. փոստի միջոցով: Բարեգործական կազմակերպությունն իր տրամադրության տակ ունի անցած տասներկու ամիսների ընթացքում կատարված նվիրատվությունների, ինչպես նաև նվիրատուների անունների և էլ. հասցեների մասին տեղեկությունները: Հսկողը կարող էր տրամադրել անձնական տվյալների և լրացուցիչ տեղեկությունների կրկնօրինակը՝ էլ. փոստին պատասխանելու միջոցով, եթե կիրառվեին բոլոր անհրաժեշտ երաշխիքները՝ հաշվի առնելով, օրինակ՝ տվյալների բնույթը:

136. Նույնիսկ այն հսկողները, որոնք մշակում են մեծ քանակությամբ տվյալներ, կարող են կիրառել տվյալներին հասանելիություն ստանալու մասին դիմումներին ընթացք տալու մեխանիկական ընթացակարգեր: Եթե հսկողը մշակում է մի շարք տարբեր գերատեսչությունների տվյալներ, ապա նա պետք է անձնական տվյալներ հավաքի յուրաքանչյուր դեպարտամենտից, որպեսզի կարողանա պատասխանել տվյալների սուբյեկտի դիմումին:

Օրինակ 24. Հսկողը նշանակում է ադմինիստրատոր՝ հասանելիություն ստանալու մասին դիմումների հետ կապված գործնական խնդիրները լուծելու համար: Դիմում ստանալու դեպքում ադմինիստրատորն էլեկտրոնային փոստով հարցում է ուղարկում կազմակերպության տարբեր դեպարտամենտներ՝ խնդրելով հավաքել տվյալների սուբյեկտին վերաբերող անձնական տվյալներ: Յուրաքանչյուր դեպարտամենտի ներկայացուցիչներն ադմինիստրատորին տալիս են իրենց դեպարտամենտի կողմից մշակված անձնական տվյալները: Այնուհետև ադմինիստրատորը բոլոր անձնական տվյալները, ինչպես նաև անհրաժեշտ լրացուցիչ տեղեկություններն ուղարկում է տվյալների սուբյեկտին, օրինակ և անհրաժեշտության դեպքում՝ էլ. փոստով:

137. Թեև հասանելիություն ստանալու մասին դիմումներին ընթացք տալու համար կիրառվող մեխանիկական գործընթացները կարող են պատշաճ համարվել, այնուամենայնիվ, որոշ հսկողներ կարող են օգտվել տվյալների սուբյեկտների դիմումներին ընթացք տալու ավտոմատացված գործընթացներից: Սա կարող է կիրառելի լինել, օրինակ՝ այն հսկողների դեպքում, որոնք ստանում են մեծ թվով դիմումներ: 15-րդ հոդվածով նախատեսված տեղեկությունների տրամադրման եղանակներից մեկը տվյալների սուբյեկտին ինքնասպասարկման գործիքներով ապահովելն է: Սա կարող է դյուրացնել տվյալների սուբյեկտների հասանելիություն ստանալու մասին դիմումներին արդյունավետ կերպով և ժամանակին ընթացք տալու գործընթացը, ինչպես նաև հնարավորություն տալ հսկողին ինքնասպասարկման գործիքի մեջ ներառել ստուգման մեխանիզմը:

Օրինակ 25. Սոցիալական ցանցերն ունեն հասանելիություն ստանալու մասին դիմումներին ընթացք տալու ավտոմատացված գործընթաց, որը հնարավորություն է տալիս տվյալների սուբյեկտին իր օգտատիրոջ հաշվից մուտք գործել անձնական տվյալներ: Անձնական տվյալներն առբերելու համար սոցիալական ցանցերի օգտատերերը կարող են ընտրել «Ներբեռնել Ձեր անձնական տվյալները» տարբերակը, երբ մուտք են գործում իրենց օգտատիրոջ հաշիվ: Ինքնասպասարկման այդ տարբերակը թույլ է տալիս օգտատերերին իրենց սեփական համակարգիչ ներբեռնել անձնական տվյալները պարունակող ֆայլ անմիջապես օգտատիրոջ հաշվից:

138. Ինքնասպասարկման գործիքների կիրառումը երբեք չպետք է սահմանափակի ստացված անձնական տվյալների շրջանակը: Եթե ինքնասպասարկման գործիքի միջոցով հնարավոր չի լինում տրամադրել 15-րդ հոդվածով նախատեսված բոլոր տեղեկությունները, ապա մնացած տեղեկությունները պետք է տրամադրվեն այլ եղանակով: Հսկողը կարող է իսկապես խրախուսել տվյալների սուբյեկտին կիրառել ինքնասպասարկման գործիք, որը նա սահմանել է հասանելիություն ստանալու մասին դիմումներին ընթացք տալու համար: Այնուամենայնիվ, հարկ է նշել, որ հսկողը պետք է ընթացք տա նաև հասանելիություն ստանալու մասին այն դիմումներին, որոնք չեն ուղարկվել հաղորդակցության հաստատված ուղիներով[78]:

5.2.3 «Հակիրճ, թափանցիկ, հասկանալի և հեշտ հասանելի ձևով՝ պարզ ու հասարակ լեզվով» հասանելիություն ապահովելը

139. ՏՊԸԿ 12(1) հոդվածի համաձայն՝ հսկողը ձեռնարկում է համապատասխան միջոցներ, որպեսզի 15-րդ հոդվածի համաձայն՝ հստակ, թափանցիկ, հասկանալի և հեշտ հասանելի ձևով՝ պարզ ու հասարակ լեզվով ապահովի հասանելիություն:

140. Տվյալների սուբյեկտին հասանելիություն ապահովելու պահանջը պետք է կատարվի հակիրճ և թափանցիկ կերպով, այսինքն՝ հսկողները պետք է տեղեկությունները ներկայացնեն արդյունավետ և համառոտ կերպով այնպես, որ տվյալների սուբյեկտը, հատկապես եթե նա երեխա է, հեշտությամբ հասկանա դրանք: Հսկողը պետք է հաշվի առնի տվյալների քանակն ու բարդությունը՝ 15-րդ հոդվածով նախատեսված հասանելիություն ապահովելու եղանակն ընտրելիս:

Օրինակ 26. Սոցիալական ցանցերի մատակարարը տվյալների սուբյեկտի մասին մշակում է մեծ քանակությամբ տեղեկություններ: Այդ անձնական տվյալների մեծ մասը լոգ ֆայլերի հարյուրավոր էջերում զետեղված տեղեկություններ են, որոնցում գրանցվում է կայքէջում տվյալների սուբյեկտի ակտիվությունը: Եթե տվյալների սուբյեկտները դիմում են իրենց անձնական տվյալներին հասանելիություն ստանալու խնդրանքով, ապա այդ լոգ ֆայլերում առկա անձնական տվյալներն իսկապես կարգավորվում են հասանելիություն ունենալու իրավունքով: Հետևաբար, հասանելիություն ունենալու իրավունքը կարող է ֆորմալ առումով իրացվել, եթե լոգ ֆայլերի այս հարյուրավոր էջերը տրամադրվեին տվյալների սուբյեկտին: Այնուամենայնիվ, առանց լոգ ֆայլերում առկա տեղեկությունները հասկանալու գործընթացը դյուրացնելու համար ձեռնարկված միջոցների, տվյալների սուբյեկտի հասանելիություն ունենալու իրավունքը կարող է գործնականում չիրացվել, քանի որ լոգ ֆայլերից որևէ տեղեկություն հնարավոր չէ հեշտությամբ դուրս բերել, ինչի արդյունքում չի կատարվում ՏՊԸԿ 12(1) հոդվածի պահանջը: Ուստի, հսկողը պետք է շրջահայաց լինի և մանրակրկիտ կերպով ընտրի տվյալների սուբյեկտին տեղեկություններ և անձնական տվյալներ ներկայացնելու եղանակը:

[78] Տե՛ս 3.1.2 բաժինը

141. Վերոնշյալ օրինակում նկարագրված հանգամանքներում գաղտնիության մասին ծանուցումների առնչությամբ Թափանցիկության վերաբերյալ ուղեցույցում ներկայացված բազմաշերտ մոտեցման նման բազմաշերտ մոտեցման կիրառումը[79] կարող է պաշտաճ միջոց լինել՝ ՏՊԸԿ 15-րդ և 12(1) հոդվածներով նախատեսված պահանջները կատարելու համար: Բազմաշերտ մոտեցման մասին լրացուցիչ տեղեկություններ կարելի է գտնել ներքոնշյալ 5.2.4 բաժնում: Տեղեկությունների «հասկանալի» լինելու պահանջը նշանակում է, որ այն պետք է հասկանալի լինի նախատեսված լսարանի համար[80]՝ միևնույն ժամանակ նկատի ունենալով տվյալների սուբյեկտի որևէ կոնկրետ պահանջ, որը հայտնի է հսկողին[81]: Քանի որ հասանելիություն ունենալու իրավունքը հաճախ հնարավորություն է տալիս իրացնել տվյալների սուբյեկտի այլ իրավունքներ, ուստի չափազանց կարևոր է, որ տրամադրված տեղեկությունները լինեն հասկանալի և հստակ: Դա պայմանավորված է նրանով, որ տվյալների սուբյեկտները կարող են դիտարկել այն հարցը, թե արդյոք օգտվեն իրենց՝ ՏՊԸԿ 16-րդ հոդվածի համաձայն, օրինակ՝ ուղղում կատարելու իրավունքից այն ժամանակ, երբ իմանան, թե ինչ անձնական տվյալներ են մշակվում, ինչ նպատակներով և այլն: Արդյունքում կարող է անհրաժեշտություն առաջանալ, որպեսզի հսկողը տվյալների սուբյեկտին տրամադրի լրացուցիչ տեղեկություններ, որոնք բացատրում են տրամադրված տվյալները: Անհրաժեշտ է ընդգծել, որ տվյալների մշակման բարդությունը պարտավորեցնում է հսկողին միջոցներ նախատեսել՝ տվյալները հասկանալի դարձնելու համար և չի կարող օգտագործվել որպես փաստարկ՝ բոլոր տվյալների հասանելիությունը սահմանափակելու համար: Նույն կերպ, տվյալները հակիրճ ձևով տրամադրելու հսկողի պարտավորությունը չի կարող օգտագործվել որպես փաստարկ՝ բոլոր տվյալներին հասանելիությունը սահմանափակելու համար:

Օրինակ 27. Էլեկտրոնային առևտրով զբաղվող կայքէջը մարքեթինգային նպատակներով հավաքում է իր կայքում դիտված կամ գնված ապրանքների մասին տվյալներ: Այս տվյալների մի մասը բաղկացած կլինի չմշակված ձևաչափով տվյալներից[82], որոնք չեն վերլուծվել և չեն կարող անմիջապես իմաստ արտահայտել ընթերցողի համար (ծածկագրեր, ակտիվության պատմություն և այլն): Տվյալների սուբյեկտների ակտիվությանը վերաբերող նմանատիպ տվյալների վրա նույնպես տարածվում է հասանելիություն ունենալու իրավունքը, հետևաբար, դրանք պետք է տրամադրվեն տվյալների սուբյեկտին՝ի պատասխան հասանելիություն ստանալու մասին դիմումի: Չմշակված ձևաչափով տվյալներ տրամադրելիս կարևոր է, որ հսկողը ձեռնարկի անհրաժեշտ միջոցներ՝ապահովելու համար, որ տվյալների սուբյեկտը հասկանա տվյալները, օրինակ՝ տրամադրելով բացատրական փաստաթուղթ, որը չմշակված ձևաչափը փոխակերպում է հեշտ կիրառելի ձևաչափի: Բացի դրանից, այդ փաստաթղթում կարող են ներկայացնել հապավումներ և կրճատումներ, ինչպես օրինակ՝ «A»-ն նշանակում է, որ գնման գործընթացն ընդհատվել է, իսկ «B»-ն նշանակում է, որ գնումն իրականացել է:

[79] ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, պարբերություն 35:

[80] Ընբռնումը սերտորեն փոխկապված է հասարակ և պարզ լեզու կիրառելու պահանջի հետ (ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույց, պարբերություն 9): ՏՊԸԿ 13-րդ և 14-րդ հոդվածներում նշված տեղեկությունների առնչությամբ 12-16-րդ պարբերություններում հասարակ և պարզ լեզվի մասին անդրադարձը հավասարապես կիրառվում է 15-րդ հոդվածի համաձայն հաղորդակցության նկատմամբ:

[81] Տե՛ս 128-րդ պարբերությունը:

[82] Օրինակի չմշակված ձևաչափը պետք է հասկանալ որպես մշակման հիմքում ընկած չվերլուծված տվյալներ, և ոչ թե չմշակված տվյալների ամենացածր մակարդակը, որոնք կարող են միայն մեքենայաընթեռնելի լինել (օրինակ՝ «բիթեր»):

142. «Հեշտ հասանելի» տարրը նշանակում է, որ 15-րդ հոդվածով նախատեսված տեղեկությունները պետք է ներկայացվեն այնպես, որ տվյալների սուբյեկտի համար դրանք լինեն հեշտ հասանելի: Դա վերաբերում է, օրինակ՝ դասավորությանը, համապատասխան վերնագրերին և պարբերություններին: Տեղեկությունները պետք է միշտ տրամադրվեն հասարակ ու պարզ լեզվով: Հսկողը, որը ծառայություններ է մատուցում որևէ այլ երկրում, պետք է պատասխանները նույնպես տրամադրի տվյալ երկրի տվյալների սուբյեկտների համար հասկանալի լեզվով: Ստանդարտացված պատկերների օգտագործումը նույնպես խրախուսվում է, երբ այն դյուրացնում է տեղեկությունների ըմբռնումն ու հասանելիությունը: Երբ տեղեկություններ ստանալու դիմումը վերաբերում է տեսողական խնդիրներ ունեցող տվյալների սուբյեկտներին կամ այլ տվյալների սուբյեկտներին, որոնք կարող են դժվարություններ ունենալ տեղեկություններին հասանելիություն ունենալու կամ դրանք հասկանալու հարցում, ակնկալվում է, որ հսկողը միջոցներ կձեռնարկի՝ դյուրացնելու տրամադրված տեղեկությունների, այդ թվում՝ բանավոր տեղեկությունների ըմբռնումը, եթե դա անհրաժեշտ է[83]: Հսկողը պետք է հատուկ ուշադրություն դարձնի, որպեսզի տարեցները, երեխաները, տեսողական խնդիրներ ունեցող անձինք կամ ճանաչողական կամ այլ տեսակի հաշմանդամություն ունեցող անձինք կարողանան իրացնել իրենց իրավունքները, օրինակ՝ պրոակտիվ կերպով նախատեսելով հեշտ հասանելի տարրեր՝ այդ իրավունքների իրացումը դյուրացնելու համար:

5.2.4 Մեծ քանակությամբ տեղեկությունները պահանջում են տեղեկությունների տրամադրման եղանակների նկատմամբ հատուկ պահանջներ

143. Անկախ հասանելիություն ապահովելու համար կիրառվող միջոցներից, կարող է հակասություն առաջանալ հսկողի կողմից տվյալների սուբյեկտներին տրամադրվելիք տեղեկությունների քանակի և դրանց հակիրճ լինելու պահանջի միջև: Երկու նպատակներին հասնելու եղանակներից մեկը և մեծ քանակությամբ տվյալներ տրամադրելու դեպքում որոշ հսկողների համար պատշաճ միջոցի օրինակը բազմաշերտ մոտեցում կիրառելն է: Այս մոտեցումը կարող է դյուրացնել տվյալների սուբյեկտների կողմից տվյալների ըմբռնումը: Այնուամենայնիվ, պետք է ընդգծել, որ այս մոտեցումը կարող է կիրառվել միայն որոշ հանգամանքներում և պետք է իրականացվի այնպես, որ չսահմանափակի հասանելիություն ունենալու իրավունքը, ինչպես ներկայացված է ստորև: Ավելին, բազմաշերտ մոտեցման կիրառումը չպետք է լրացուցիչ բեռ ստեղծի տվյալների սուբյեկտի համար: Հետևաբար, լավ կլինի, որ հասանելիությունն ապահովվի առցանց միջավայրում: Բազմաշերտ մոտեցումը պարզապես միջոց է 15-րդ հոդվածով նախատեսված տեղեկություններն այնպես ներկայացնելու, որը նույնպես համապատասխանում է ՏՊԸԿ 12(1) հոդվածի պահանջներին և չպետք է շփոթել հսկողների՝ տվյալների սուբյեկտից այնպիսի տեղեկությունների կամ մշակման գործողությունների հստակեցում պահանջելու հնարավորության հետ, որին դիմումը վերաբերում է՝ ՏՊԸԿ 63-րդ ներածական դրույթով սահմանված կարգով[84]:

---

[83] Տե՛ս ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույցը, պարբերություն 21:

[84] Տե՛ս նաև 2.3.1 բաժինը:

144. Հասանելիություն ունենալու իրավունքի առնչությամբ կիրառվող բազմաշերտ մոտեցումը նշանակում է, որ հսկողը, որոշ հանգամանքներում, կարող է տարբեր մակարդակներով տրամադրել 15-րդ հոդվածով պահանջվող անձնական տվյալներն ու լրացուցիչ տեղեկությունները: Առաջին մակարդակը պետք է ներառի 15(1)(ա)-(ը) և 15(2) հոդվածի համաձայն՝ մշակման և տվյալների սուբյեկտի իրավունքների մասին տեղեկություններ, ինչպես նաև մշակված անձնական տվյալների առաջին մասը: Երկրորդ մակարդակում պետք է տրամադրվեն առավել շատ անձնական տվյալներ:

145. Տարբեր մակարդակներում տրամադրման ենթակա տեղեկությունների տեսակների վերաբերյալ որոշում կայացնելիս հսկողը պետք է հաշվի առնի, թե տվյալների սուբյեկտը, ընդհանուր առմամբ, որ տեղեկությունները կհամարի առավել կարևոր: Արդարության սկզբունքին համապատասխան՝ առաջին մակարդակը նույնպես պետք է պարունակի մշակման վերաբերյալ տեղեկություններ, որոնք ամենամեծ ազդեցությունն ունեն տվյալների սուբյեկտի վրա[85]: Հսկողները պետք է կարողանան պատասխանատվություն կրել՝ վերը նշվածի վերաբերյալ իրենց հիմնավորման համար:

Օրինակ 28. Հսկողը վերլուծում է տվյալների մեծ հավաքածուներ, որպեսզի հաճախորդների առցանց վարքագծից ելնելով կարողանա նրանց բաշխել տարբեր սեգմենտներում: Այս դեպքում կարելի է ենթադրել, որ տվյալների սուբյեկտների համար ամենակարևորն այն մասին տեղեկություններ ստանալն է, թե որ սեգմենտում են նրանք գտնվում: Արդյունքում, այդ տեղեկությունները պետք է ներառվեն առաջին մակարդակում: Չմշակված ձևաչափով տվյալները[86], որոնք դեռևս չեն վերլուծվել կամ լրացուցիչ մշակում չեն անցել, օրինակ՝ օգտատերերի ակտիվությունը կայքէջում, նույնպես համարվում են հասանելիություն ունենալու իրավունքով կարգավորվող անձնական տվյալներ, սակայն որոշ դեպքերում կարող է բավարար լինել այդ տեղեկությունները տրամադրել մեկ այլ մակարդակում:

[85] Տե՛ս ՏՊԵԽ-ի կողմից հաստատված՝ Թափանցիկության վերաբերյալ 29-րդ հոդվածով սահմանված աշխատանքային խմբի ուղեցույցը, պարբերություն 36:
[86] Տե՛ս 82-րդ տողատակի ծանոթագրությունը:

146. Բազմաշերտ մոտեցման կիրառումը պատշաճ միջոց համարվելու համար անհրաժեշտ է, որ տվյալների սուբյեկտն ի սկզբանե տեղեկացված լինի, որ 15-րդ հոդվածով նախատեսված տեղեկությունները համակարգված են տարբեր մակարդակներով և նկարագրությամբ, թե տարբեր մակարդակներում ինչ անձնական տվյալներ և տեղեկություններ կպարունակվեն: Այս կերպ տվյալների սուբյեկտի համար ավելի հեշտ կլինի որոշել, թե որ մակարդակին է ցանկանում հասանելիություն ստանալ: Նկարագրությունը պետք է օբյեկտիվորեն արտացոլի անձնական տվյալների այն բոլոր կատեգորիաները, որոնք փաստացի մշակվում են հսկողի կողմից: Պետք է նաև պարզ լինի, թե տվյալների սուբյեկտն ինչպես կարող է հասանելիություն ստանալ տարբեր մակարդակներին: Տարբեր մակարդակների հասանելիությունը չի հանգեցնում տվյալների սուբյեկտի համար անհամաչափ ջանքերի գործադրման և պայմանավորված չէ տվյալների սուբյեկտի կողմից նոր դիմում ներկայացնելով: Սա նշանակում է, որ տվյալների սուբյեկտները պետք է հնարավորություն ունենան ընտրելու, թե արդյոք հասանելիություն ստանան բոլոր մակարդակներին միանգամից, թե մեկ կամ երկու մակարդակներին, եթե դա նրանց համար բավարար է:

Օրինակ 29. Տվյալների սուբյեկտը տեսանյութերի հոսքային ծառայությանը հասանելիություն ստանալու մասին դիմում է ներկայացնում: Դիմումը ներկայացվում է այն տարբերակի միջոցով, որը հասանելի է դառնում, երբ տվյալների սուբյեկտները մուտք են գործել իրենց հաշիվներ: Տվյալների սուբյեկտին առաջարկվում է երկու տարբերակ, որոնք հայտնվում են կայքէջում կոճակների տեսքով: Առաջին տարբերակն անձնական տվյալների 1-ին մասի և լրացուցիչ տեղեկությունների ներբեռնումն է: Սա ներառում է, օրինակ՝ վերջին հոսքային հաղորդման պատմությունը, հաշվի և վճարման մասին տեղեկությունները: Երկրորդ տարբերակը տվյալների սուբյեկտների ակտիվության մասին տեխնիկական լոգ ֆայլեր և հաշվի վերաբերյալ արխիվային տեղեկություններ պարունակող անձնական տվյալների 2-րդ մասի ներբեռնումն է: Այս դեպքում հսկողը հնարավորություն է տվել տվյալների սուբյեկտներին իրացնել իրենց իրավունքն այնպես, որ լրացուցիչ բեռ չստեղծվի տվյալների սուբյեկտի համար:

Տարբերակ 1. Այն դեպքերում, երբ տվյալների սուբյեկտն ընտրում է միայն անձնական տվյալների 1-ին մասը ներբեռնելու կոճակը, հսկողը պարտավոր է տրամադրել տվյալների միայն 1-ին մասը:

Տարբերակ 2. Այն դեպքերում, երբ տվյալների սուբյեկտն ընտրում է տվյալների և 1-ին ու 2-րդ մասի կոճակները, հսկողը չի կարող փոխանցել տվյալների միայն 1-ին մասը և պահանջել նոր հաստատում մինչև տվյալների 2-րդ մասը փոխանցելը: Փոխարենը տվյալների սուբյեկտին պետք է տրամադրվեն տվյալների երկու մասերը, ինչպես հայցվում է ներկայացված դիմումի մեջ:

147. Բազմաշերտ մոտեցման կիրառումը պատշաճ չի համարվի բոլոր հսկողների համար կամ բոլոր իրավիճակներում: Այն պետք է կիրառվի միայն այն դեպքում, երբ տվյալների սուբյեկտի համար դժվար կլինի հասկանալ տեղեկությունները, եթե դրանք ամբողջությամբ տրամադրվեն: Այլ կերպ ասած, հսկողը պետք է կարողանա ապացուցել, որ բազմաշերտ մոտեցման կիրառումը հավելյալ արժեք է ստեղծում տվյալների սուբյեկտի համար՝ օգնելով նրանց հասկանալ տրամադրված տեղեկությունները: Հետևաբար, բազմաշերտ մոտեցման կիրառումը պատշաճ կհամարվի միայն այն դեպքում, երբ հսկողը մշակում է դիմում ներկայացրած տվյալների սուբյեկտի վերաբերյալ մեծ քանակությամբ անձնական տվյալներ, և երբ տվյալների սուբյեկտի համար կան տեղեկություններն ընկալելու կամ ըմբռնելու ակնհայտ դժվարություններ, եթե դրանք տրամադրվեն ամբողջությամբ և միանգամից: Այն փաստը, որ հսկողից մեծ ջանքեր և ռեսուրսներ կպահանջվեն 15-րդ հոդվածով նախատեսված տեղեկությունները տրամադրելու համար, ինքնին փաստարկ չէ՝ բազմաշերտ մոտեցում կիրառելու համար:

5.2.5 Ձևաչափը

148. Համաձայն ՏՊԸԿ 12(1) հոդվածի՝ 15-րդ հոդվածով նախատեսված տեղեկությունները տրամադրվում են գրավոր կամ այլ միջոցներով, այդ թվում, եթե անհրաժեշտ է, ապա էլեկտրոնային միջոցներով: Ինչ վերաբերում է մշակվող անձնական տվյալների հասանելիությանը՝ 15(3) հոդվածով նշվում է, որ եթե տվյալների սուբյեկտը դիմումը ներկայացնում է էլեկտրոնային միջոցներով, և եթե տվյալների սուբյեկտն այլ բան չի պահանջում, ապա տեղեկությունները տրամադրվում են լայնորեն կիրառվող էլեկտրոնային եղանակով: ՏՊԸԿ-ով չի նշում, թե որն է լայնորեն կիրառվող էլեկտրոնային եղանակը: Այսպիսով, գոյություն ունեն մի քանի հնարավոր ձևաչափեր, որոնք կարող են կիրառվել: Թե, ինչն է համարվում լայնորեն կիրառվող էլեկտրոնային եղանակ, նույնպես կփոփոխվի ժամանակի ընթացքում:

149. Այն, ինչը կարող է համարվել լայնորեն կիրառվող էլեկտրոնային եղանակ, պետք է հիմնված լինի օբյեկտիվ գնահատման, այլ ոչ թե նրա վրա, թե ինչ ձևաչափ է կիրառում հսկողն իր ամենօրյա գործունեության մեջ: Որոշելու համար, թե որ ձևաչափը պետք է դիտարկվի լայնորեն կիրառվող ձևաչափ տվյալ դեպքում, հսկողը պետք է գնահատի, թե արդյոք կան հատուկ ձևաչափեր, որոնք սովորաբար կիրառվում են հսկողի գործունեության ոլորտում կամ տվյալ համատեքստում: Երբ չկան լայնորեն կիրառվող նման ձևաչափեր, միջազգային ստանդարտով՝ ISO-ով սահմանված բաց ձևաչափերը, պետք է ընդհանուր առմամբ համարվեն լայնորեն կիրառվող էլեկտրոնային ձևաչափեր: Այնուամենայնիվ, ՏՊԵԽ-ը չի բացառում, որ այլ ձևաչափեր նույնպես կարող են 15(3) հոդվածի իմաստով համարվել լայնորեն կիրառվող ձևաչափեր: Գնահատելիս, թե արդյոք ձևաչափը սովորաբար լայնորեն կիրառվող էլեկտրոնային ձևաչափ է, ՏՊԵԽ-ը գտնում է, որ կարևոր է, թե որքան հեշտ անձը կարող է հասանելիություն ստանալ ընթացիկ ձևաչափով տրամադրված տեղեկություններին: Այս առումով պետք է նշել, թե ինչ տեղեկություններ է հսկողը տրամադրել տվյալների սուբյեկտին այն մասին, թե ինչպես մուտք գործել կոնկրետ ձևաչափով ֆայլ, օրինակ՝ ինչ ծրագրեր կամ ծրագրային ապահովումներ, որոնք կարող են օգտագործվել՝ ձևաչափը տվյալների սուբյեկտի համար առավել հասանելի դարձնելու համար: Այնուամենայնիվ, տվյալների սուբյեկտը չպետք է պարտավորված լինի գնել ծրագրային ապահովում՝ տեղեկություններին հասանելիություն ստանալու համար:

150. 15-րդ հոդվածով նախատեսված անձնական տվյալների և տեղեկությունների կրկնօրինակը տրամադրելու ձևաչափի ընտրության առնչությամբ որոշում կայացնելիս հսկողը պետք է նկատի ունենա, որ ձևաչափը պետք է հնարավորություն տա, որպեսզի տեղեկությունները ներկայացվեն ինչպես հասկանալի, այնպես էլ հեշտ հասանելի եղանակով: Կարևոր է, որ տվյալների սուբյեկտին տեղեկությունները տրամադրվեն ներկառուցված, մշտական ձևով (տեքստային, էլեկտրոնային): Քանի որ տեղեկությունները պետք է պահպանվեն ժամանակի ընթացքում, գրավոր, այդ թվում՝ էլեկտրոնային միջոցներով տեղեկությունները սկզբունքորեն նախընտրելի են այլ եղանակներից: Անձնական տվյալների կրկնօրինակը, հարկ եղած դեպքում, կարող է պահվել էլեկտրոնային հիշողության սարքի, ինչպես օրինակ՝ CD-ի կամ USB-ի վրա:

151. Հարկ է նշել, որ որպեսզի հսկողը կարողանա համարել, որ անձնական տվյալների կրկնօրինակը տրամադրվել է տվյալների սուբյեկտներին, բավարար չէ նրանց ապահովել անձնական տվյալներին հասանելիություն: Անձնական տվյալների

կրկնօրինակը տրամադրելու պահանջը կատարելու համար, ինչպես նա եթե տվյալները տրամադրվում են էլեկտրոնային/թվային եղանակով, տվյալների սուբյեկտները պետք է կարողանան ներբեռնել իրենց տվյալները լայնորեն կիրառվող էլեկտրոնային եղանակով:

152. Հսկողի պարտականությունն է որոշել այն պատշաճ եղանակը, որով տրամադրվելու են անձնական տվյալները: Հսկողը կարող է, թեև պարտավորված չէ, տրամադրել բնօրինակ փաստաթղթերը, որոնք պարունակում են դիմում ներկայացնող տվյալների սուբյեկտի վերաբերյալ անձնական տվյալներ: Հսկողը կարող է, օրինակ՝ յուրաքանչյուր դեպքի հիման վրա, հասանելիություն ապահովել որպես այդպիսին կրիչի կրկնօրինակին՝ հաշվի առնելով թափանցիկության անհրաժեշտությունը (օրինակ՝ ստուգելու հսկողի տիրապետման տակ գտնվող տվյալների ճշգրտությունը հիվանդության պատմությանը կամ այն աուդիո ձայնագրությանը հասանելիություն ստանալու մասին դիմում ներկայացնելու դեպքում, որի վերծանումը վիճարկված է): Այնուամենայնիվ, ԵՄԱԴ-ը, 95/46/ԵՀ հրահանգով նախատեսված հասանելիություն ունենալու իրավունքի իր մեկնաբանման մեջ նշել է, որ *«[հասանելիություն ունենալու իրավունքը]* կատարելու համար բավարար է, որպեսզի դիմողին տրամադրվի տվյալների ամբողջական ամփոփագիր հասկանալի եղանակով, այսինքն՝ այնպիսի եղանակով, որը թույլ է տալիս նրան ծանոթանալ այդ տվյալներին և ստուգել, թե արդյոք դրանք ճշգրիտ են և մշակված են այդ հրահանգին համապատասխան, որպեսզի նա, հարկ եղած դեպքում, կարողանա իրացնել իրեն վերապահված իրավունքները»:[87] Բացի հրահանգից, ՏՊԸԿ-ով ուղղակիորեն սահմանվում է մշակվող անձնական տվյալների կրկնօրինակը տվյալների սուբյեկտին տրամադրելու պարտավորություն: Այնուամենայնիվ, սա չի նշանակում, որ տվյալների սուբյեկտը միշտ իրավունք ունի ստանալու անձնական տվյալներ պարունակող փաստաթղթերի օրինակը, այլ այդ փաստաթղթերում մշակվող անձնական տվյալների չփոփոխված կրկնօրինակը:[88] Անձնական տվյալների այդ օրինակները կարող են տրամադրվել հասանելիություն ունենալու իրավունքով կարգավորվող բոլոր անձնական տվյալները պարունակող հավաքածուի տեսքով, քանի դեռ այդ տվյալների հավաքածուն հնարավորություն է տալիս տվյալների սուբյեկտին տեղեկացված լինել և ստուգել մշակման օրինականությունը: Հետևաբար, այս հարցի առնչությամբ ՏՊԸԿ ձևակերպման և ԵՄԱԴ-ի որոշման միջև որևէ հակասություն չկա: Որոշման մեջ «ամփոփագիր» բառը չպետք է սխալ մեկնաբանվի, որ նշանակի, որ տվյալների հավաքածուն չի պարունակում հասանելիություն ունենալու իրավունքով կարգավորվող բոլոր տվյալները, այլ ընդամենը մի միջոց է՝ ներկայացնելու բոլոր այդ տվյալները՝ առանց անձնական տվյալներ պարունակող հիմնական փաստաթղթերին հասանելիություն ապահովելու: Քանի որ տվյալների հավաքածուն պետք է պարունակի անձնական տվյալների կրկնօրինակը, անհրաժեշտ է ընդգծել, որ այն պետք է կազմվի այնպես, որ որևէ կերպ չփոփոխվի կամ փոխի տեղեկությունների բովանդակությունը:

---

[87] ԵՄԱԴ, թիվ C-141/12 և թիվ C-372/12 միացված գործեր, *Ուայէսը և այլք գործ*, պարբերություն 60:

[88] Այս թեմային առնչվող հարցերը հանդիսանում են ԵՄԱԴ-ում ներկայումս քննվող գործի քննության առարկա (թիվ C-487/21 և թիվ C-307/21 գործեր):

Օրինակ 30. Տվյալների սուբյեկտը երկար տարիներ ապահովագրված է եղել ապահովագրական ընկերությունում: Տեղի են ունեցել մի շարք ապահովագրական միջադեպեր: Յուրաքանչյուր դեպքում տվյալների սուբյեկտի և ապահովագրական ընկերության միջև էլ. փոստով տեղի է ունեցել գրավոր նամակագրություն: Քանի որ տվյալների սուբյեկտը պետք է տեղեկություններ տրամադրեր յուրաքանչյուր միջադեպի կոնկրետ հանգամանքների առնչությամբ, ուստի, նամակագրությունը պարունակում է տվյալների սուբյեկտի վերաբերյալ (սիրած զբաղմունքներ, հարևաններ, առօրյա սովորություններ և այլն) բազմաթիվ անձնական տեղեկություններ: Որոշ դեպքերում ապահովագրական ընկերության կողմից տվյալների սուբյեկտին փոխհատուցելու պարտավորության առնչությամբ տարաձայնություններ են առաջացել, որի արդյունքում տեղի է ունեցել մեծ թվով փոխադարձ հաղորդակցություն: Այս ամբողջ նամակագրությունը պահվում է ապահովագրական ընկերության կողմից: Տվյալների սուբյեկտը հասանելիություն ստանալու մասին դիմում է ներկայացնում: Այս իրավիճակում պարտադիր չէ, որ հսկողը տրամադրի սկզբնական էլ. նամակները՝ դրանք փոխանցելով տվյալների սուբյեկտին: Փոխարենը հսկողը կարող է որոշել մեկ ֆայլի մեջ հավաքել տվյալների սուբյեկտի անձնական տվյալները պարունակող էլ. փոստի նամակագրությունը, որը կտրամադրվի տվյալների սուբյեկտին:

153. Անկախ հսկողի կողմից անձնական տվյալների տրամադրման ձևից, օրինակ՝ անձնական տվյալներ պարունակող փաստացի փաստաթղթերի կամ անձնական տվյալների հավաքածուի միջոցով, տեղեկությունները պետք է համապատասխանեն ՏՊԸԿ 12-րդ հոդվածով սահմանված թափանցիկության պահանջներին: Տվյալների որոշ հավաքածու կազմելը և (կամ) տվյալների դուրսբերումն այնպես, որ տեղեկությունները հեշտ ըմբռնելի լինեն, որոշ դեպքերում կարող է լինել այդ պահանջները կատարելու միջոց: Այլ դեպքերում տեղեկություններն ավելի լավ են ընկալվում անձնական տվյալներ պարունակող փաստացի փաստաթղթի օրինակը տրամադրելու միջոցով: Հետևաբար, տվյալների տրամադրման ձևի նպատակահարմարությունը պետք է որոշվի յուրաքանչյուր առանձին դեպքի հիման վրա:

154. Այս համատեքստում կարևոր է հիշել, որ առկա է ՏՊԸԿ 15-րդ հոդվածով նախատեսված հասանելիություն ստանալու իրավունքի և ազգային իրավունքով կարգավորվող վարչական փաստաթղթերի օրինակն ստանալու իրավունքի միջև տարբերություն, իսկ վերջինս փաստացի փաստաթղթի օրինակն ստանալու իրավունք է: Սա չի նշանակում, որ ՏՊԸԿ 15-րդ հոդվածով նախատեսված հասանելիություն ունենալու իրավունքը բացառում է այն փաստաթղթի/կրիչի օրինակն ստանալու հնարավորությունը, որի վրա առկա են անձնական տվյալներ:

155. Որոշ դեպքերում անձնական տվյալներն իրենց բնույթով են սահմանում այն պահանջները, թե ինչ ձևաչափով պետք է դրանք տրամադրվեն: Օրինակ, երբ անձնական տվյալներն իրենցից ներկայացնում են տվյալների սուբյեկտի ձեռագիր տեղեկություններ, տվյալների սուբյեկտին կարող է անհրաժեշտ լինել տրամադրել այդ ձեռագիր տեղեկությունների պատճեն, քանի որ ձեռագիրն ինքնին հանդիսանում է անձնական տվյալ: Դա հատկապես կարող է լինել այն դեպքում, երբ ձեռագիրը կարևորություն է ներկայացնում մշակման համար, օրինակ՝ Սուրբ գրությունների վերլուծությունը: Նույնը, ընդհանուր առմամբ, վերաբերում է նաև ձայնագրություններին, քանի որ տվյալների սուբյեկտի ձայնն ինքնին անձնական տվյալ է: Այնուամենայնիվ, որոշ դեպքերում, հասանելիություն կարող է ապահովվել երկխոսության վերծանումը տրամադրելու միջոցով, օրինակ, եթե դա համաձայնեցվել է տվյալների սուբյեկտի և հսկողի միջև:

156. Հարկ է նշել, որ ձևաչափի պահանջների վերաբերյալ դրույթները տարբեր են հասանելիություն ունենալու իրավունքի և տվյալների տեղափոխելիության իրավունքի առումով: Թեև ՏՊԸԿ 20-րդ հոդվածով նախատեսված տվյալների տեղափոխելիության իրավունքով պահանջվում է, որ տեղեկությունները տրամադրվեն մեքենայաընթեռնելի ձևաչափով, այնուամենայնիվ, 15-րդ հոդվածով նախատեսված տեղեկություններ ստանալու իրավունքով նման բան չի պահանջվում: Հետևաբար, այն ձևաչափերը, որոնք նպատակահարմար չեն համարվում տվյալների տեղափոխելիության մասին դիմումը բավարարելիս, օրինակ՝ pdf ֆայլերը, կարող են դեռևս նպատակահարմար լինել հասանելիություն ստանալու մասին դիմումը բավարարելիս:

5.3 Հասանելիություն ապահովելու ժամկետները

157. ՏՊԸԿ 12(3) հոդվածով պահանջվում է, որ հսկողը տվյալների սուբյեկտին տեղեկություններ տրամադրի 15-րդ հոդվածին համապատասխան դիմումի առնչությամբ ձեռնարկված գործողությունների մասին առանց անհարկի ձգձգումների և ցանկացած դեպքում դիմումն ստանալուց հետո մեկ ամսվա ընթացքում: Այս վերջնաժամկետը կարող է երկարաձգվել առավելագույնը երկու ամսով՝ հաշվի առնելով դիմումների բարդությունն ու քանակը, եթե տվյալների սուբյեկտը տեղեկացված է այդ ձգձգման պատճառների մասին դիմումն ստանալուց հետո մեկ ամսվա ընթացքում: Ժամկետի երկարաձգման և դրա պատճառների մասին տվյալների սուբյեկտին տեղեկացնելու այս պարտավորությունը չպետք է շփոթել այն տեղեկությունների հետ, որոնք պետք է տրամադրվեն առանց ձգձգման և ամենաուշը մեկ ամսվա ընթացքում, երբ հսկողը որևէ գործողություն չի ձեռնարկում դիմումի առնչությամբ՝ ՏՊԸԿ 12(4) հոդվածով սահմանված կարգով:

158. Հսկողը պետք է արձագանքի և, որպես կանոն, տրամադրի 15-րդ հոդվածով նախատեսված տեղեկություններն առանց անհարկի ձգձգումների, ինչը նշանակում է, որ տեղեկությունները պետք է տրամադրվեն որքան հնարավոր է շուտ: Սա նշանակում է, որ եթե հնարավոր է պահանջվող տեղեկությունները տրամադրել մեկ ամսից ավելի կարճ ժամկետում, ապա հսկողը պետք է դրանք տրամադրի ավելի վաղ: ՏՊԵԽ-ը համարում է նաև, որ որոշ դեպքերում դիմումին պատասխանելու ժամկետը պետք է համապատասխանեցվի պահպանման ժամկետին, որպեսզի հնարավոր լինի ապահովել հասանելիություն[89]:

[89] Տե՛ս 2.3.3 բաժինը:

159. Ժամկետի հաշվարկը սկսվում է այն պահից, երբ հսկողը ստանում է 15-րդ հոդվածով նախատեսված դիմումը, ինչը նշանակում է, որ դիմումը հասնում է հսկողին պաշտոնական խողովակներից որևէ մեկի միջոցով:[90] Պարտադիր չէ, որ հսկողն իրականում տեղյակ լինի դիմումի մասին: Այնուամենայնիվ, երբ հսկողը ստիպված է հաղորդակցվել տվյալների սուբյեկտի հետ՝ դիմում ներկայացնող անձի ինքնության հետ կապված անորոշությունների պատճառով, ժամանակի հաշվարկը կարող է կասեցվել մինչև հսկողը տվյալների սուբյեկտից ձեռք բերի անհրաժեշտ տեղեկությունները՝ պայմանով, որ նա լրացուցիչ տեղեկություններ ձեռք է բերել առանց անհարկի ձգձգման: Նույնը վերաբերում է այն դեպքին, երբ հսկողը դիմել է տվյալների սուբյեկտին խնդրանքով հստակեցնել այն մշակման գործողությունները, որոնց վերաբերում է դիմումը, երբ 63-րդ ներածական դրույթում նշված պայմանները բավարարված են[91]:

Օրինակ 31. Դիմումն ստանալուց հետո հսկողն անմիջապես արձագանքում է և խնդրում իրեն տրամադրել այն տեղեկությունները, որոնք անհրաժեշտ են՝ դիմում ներկայացնող անձի ինքնությունը հաստատելու համար: Վերջինս պատասխանում է միայն մի քանի օր անց, և այն տեղեկությունները, որոնք տվյալների սուբյեկտն ուղարկում է ինքնությունը ստուգելու համար, բավարար չեն համարվում, ինչը ստիպում է հսկողին դիմել՝ պարզաբանումներ ստանալու խնդրանքով: Այս դեպքում ժամկետը կասեցվում է, քանի դեռ հսկողը բավարար տեղեկություններ ձեռք չի բերել՝ տվյալների սուբյեկտի ինքնությունը ստուգելու համար:

160. Հասանելիություն ստանալու մասին դիմումին պատասխանելու ժամկետը պետք է հաշվարկվի թիվ 1182/71 կանոնակարգին համապատասխան[92]:

Օրինակ 32. Կազմակերպությունը դիմում է ստանում մարտի 5-ին: Ժամկետի հաշվարկը սկսվում է նույն օրվանից: Սա հնարավորություն է տալիս կազմակերպությանը դիմումը բավարարել ամենաուշը մինչև ապրիլի 5-ը ներառյալ:

Օրինակ 33. Եթե կազմակերպությունը դիմում է ստանում օգոստոսի 31-ին, և քանի որ հաջորդ ամիսն ավելի կարճ է, ապա դիմումին պատասխանելու համապատասխան ամսաթիվ գոյություն չունի, ուստի, պատասխանը տրամադրելու ամսաթիվն ամենաուշը հաջորդ ամսվա վերջին օրն է, հետևաբար՝ սեպտեմբերի 30-ը:

[90] Որոշ անդամ պետությունների ազգային իրավունքով սահմանվում է դրույթ, որով որոշվում է, թե երբ պետք է հաղորդագրությունը համարվի ստացված՝ հաշվի առնելով հանգստյան օրերը և ազգային տոները:

[91] Տե՛ս նաև 2.3.1 բաժինը:

[92] Ժամանակահատվածների, ամսաթվերի և ժամկետների նկատմամբ կիրառելի կանոններ սահմանող՝ Խորհրդի 1971 թվականի հունիսի 3-ի թիվ 1182/71 կանոնակարգ (ԵՏՀ, Եվրատոմ

161. Եթե այս ժամկետի վերջին օրը հանգստյան օր է կամ պետական տոն, ապա հսկողը կարող է դիմումին պատասխանել այդ օրվան հաջորդող աշխատանքային օրը:

162. Որոշ դեպքերում, եթե կա դրա անհրաժեշտությունը, հսկողը կարող է հասանելիություն ստանալու մասին դիմումին պատասխանելու ժամկետը երկարաձգել ևս երկու ամսով՝ հաշվի առնելով դիմումների բարդությունն ու քանակը: Հարկ է ընդգծել, որ այս հնարավորությունը բացառություն է ընդհանուր կանոնից և չպետք է անհարկի օգտագործվի: Եթե հսկողները հաճախ ստիպված են լինում երկարաձգել ժամկետը, ապա դա կարող է վկայել դիմումներին ընթացք տալու իրենց ընդհանուր ընթացակարգերի լրամշակման անհրաժեշտության մասին:

163. Դիմումը համարվում է բարդ՝ ելնելով յուրաքանչյուր գործի կոնկրետ հանգամանքներից: Որոշ գործոններ, որոնք կարող են կարևոր համարվել, հետևյալն են.

- հսկողի կողմից մշակվող տվյալների քանակը
- տեղեկությունների պահպանման եղանակը, հատկապես, երբ դժվար է դրանք առբերել, օրինակ, երբ տվյալները մշակվում են կազմակերպության տարբեր ստորաբաժանումների կողմից
- բացառություն կիրառվելու դեպքում տեղեկությունները, օրինակ՝ այլ տվյալների սուբյեկտների վերաբերյալ տեղեկությունները կամ առևտրային գաղտնիք կազմող տեղեկությունները խմբագրելու անհրաժեշտությունը, և
- երբ տեղեկությունները լրացուցիչ մշակման կարիք ունեն՝ հասկանալի դառնալու համար:

164. Միայն այն փաստը, որ դիմումը բավարարելը մեծ ջանքեր է պահանջում, դիմումը չի դարձնում բարդ: Նույն կերպ, այն փաստը, որ մեծ ընկերությունը ստանում է մեծ թվով դիմումներ, ավտոմատ կերպով չի հանգեցնում ժամկետի երկարաձգման: Այնուամենայնիվ, երբ հսկողը ժամանակավորապես ստանում է մեծ քանակությամբ դիմումներ, օրինակ՝ իր գործունեության առնչությամբ չափազանց մեծ հեղինակության պատճառով, դա կարող է համարվել պատասխանի ժամկետը երկարաձգելու իրավաչափ պատճառ: Այնուամենայնիվ, հսկողը, հատկապես նա, ով մեծ քանակությամբ տվյալներ է մշակում, պետք է ունենա ընթացակարգեր և մեխանիզմներ, որպեսզի սովորական պայմաններում կարողանա սահմանված ժամկետում ընթացք տալ դիմումներին:

6 ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ ՈՒՆԵՆԱԼՈՒ ԻՐԱՎՈՒՆՔԻ ՍԱՀՄԱՆՆԵՐՆ ՈՒ ՍԱՀՄԱՆԱՓԱԿՈՒՄՆԵՐԸ

6.1 Ընդհանուր դիտարկումները

165. Հասանելիություն ունենալու իրավունքի նկատմամբ գործում են ՏՊԸԿ 15(4) հոդվածով (այլ անձանց իրավունքներն ու ազատությունները) և ՏՊԸԿ 12(5) հոդվածով (ակնհայտորեն անհիմն կամ սահմազանցող դիմումներ) նախատեսված սահմանները: Ավելին, Միության կամ անդամ պետությունների իրավունքը կարող է սահմանափակել հասանելիություն ունենալու իրավունքը՝ ՏՊԸԿ 23-րդ հոդվածին համապատասխան: Գիտական, պատմական հետազոտությունների կամ վիճակագրական կամ հանրային շահերից ելնելով՝ արխիվացման նպատակներով անձնական տվյալների մշակման մասով

շեղումները կարող են հիմնվել համապատասխանաբար ՏՊԸԿ 89(2) և 89(3) հոդվածների վրա, իսկ լրագրողական նպատակներով կամ ակադեմիական, գեղարվեստական կամ գրական նպատակով մշակման մասով շեղումները՝ ՏՊԸԿ 85(2) հոդվածի վրա:

166. Կարևոր է նշել, որ, բացի վերը նշված սահմաններից, շեղումներից և հնարավոր սահմանափակումներից, ՏՊԸԿ-ով արգելվում են հասանելիություն ունենալու իրավունքից ցանկացած այլ բացառություններ կամ շեղումներ: Դա նշանակում է, որ *ի թիվս այլնի* հասանելիություն ունենալու իրավունքից որևէ ընդհանուր վերապահում՝ կապված այն ջանքերի համաչափության հետ, որոնք հսկողը պետք է ձեռնարկի տվյալների սուբյեկտների դիմումը բավարարելու համար, չի կատարվում՝ համաձայն ՏՊԸԿ 15-րդ հոդվածի[93]: Ավելին, արգելվում է հսկողի և տվյալների սուբյեկտի միջև կնքվող պայմանագրով սահմանել հասանելիություն ունենալու իրավունքի սահմանները կամ սահմանափակել այն:

167. Համաձայն 63-րդ ներածական դրույթի՝ հասանելիություն ունենալու իրավունքը տրամադրվում է տվյալների սուբյեկտներին, որպեսզի նրանք իմանան, թե արդյոք իրենց տվյալները մշակվում են և մշակվելու դեպքում ստուգել դրա օրինականությունը: Հասանելիություն ունենալու իրավունքը, *ի թիվս այլնի*, հնարավորություն է տալիս տվյալների սուբյեկտին, կախված հանգամանքներից, կատարել անձնական տվյալների ուղղում, ոչնչացում կամ ուղափեկում[94]: Այնուամենայնիվ, տվյալների սուբյեկտները պարտավոր չեն պատճառներ ներկայացնել կամ հիմնավորել իրենց դիմումը: Քանի դեռ ՏՊԸԿ 15-րդ հոդվածի պահանջները բավարարվում են, դիմումի նպատակները պետք է համարվեն ոչ էական[95]:

6.2 ՏՊԸԿ 15(4) հոդվածը

168. ՏՊԸԿ 15(4) հոդվածի համաձայն՝ կրկնօրինակը ձեռք բերելու իրավունքը չպետք է բացասաբար անդրադառնա այլ անձանց իրավունքների ու ազատությունների վրա: Այդ սահմանափակման առնչությամբ պարզաբանումները ներկայացված են 63-րդ ներածական դրույթի հինգերորդ և վեցերորդ նախադասություններում: Այդ իրավունքը չպետք է բացասաբար անդրադառնա այլ անձանց իրավունքների կամ ազատությունների վրա, այդ թվում՝ առևտրային գաղտնիքների կամ մտավոր սեփականության և, մասնավորապես՝ հեղինակային իրավունքի վրա, որով պաշտպանված են ծրագրային ապահովումները: Այնուամենայնիվ, այդ նկատառումների արդյունքում չպետք է մերժվի տվյալների սուբյեկտին բոլոր տեղեկությունների տրամադրումը: ՏՊԸԿ 15(4) հոդվածը մեկնաբանելիս անհրաժեշտ է հատուկ զգուշություն դրսևորել ՏՊԸԿ 23-րդ հոդվածով սահմանված սահմանափակումներն անհիմն կերպով չընդլայնելու համար, ինչը թույլատրելի է միայն սակավաթիվ դեպքերում:

---

[93] Եթե հսկողը մշակում է ՏՊԸԿ 63-րդ ներածական դրույթում նշված՝ տվյալների սուբյեկտին վերաբերող մեծ քանակությամբ տեղեկություններ, ապա նա կարող է դիմել տվյալների սուբյեկտին խնդրանքով հստակեցնել այն տեղեկությունները կամ մշակման գործողությունները, որոնց վերաբերում է դիմումը: Տե՛ս նաև 2.3.1 բաժինը:

[94] ԵՄԱԴ, թիվ C-141/12 և թիվ C-372/12 միացված գործեր, Ուայէսը և այլք:

[95] Սա չի հակասում ցանկացած կիրառելի ազգային իրավունքին, որը համապատասխանում է ՏՊԸԿ 23-րդ հոդվածով սահմանված պահանջներին, տե՛ս 6.4 գլուխը:

169. ՏՊԸԿ 15(4) հոդվածը կիրառվում է տվյալների կրկնօրինակը ձեռք բերելու իրավունքի նկատմամբ, որը մշակված տվյալներին հասանելիություն ապահովելու հիմնական մեթոդն է (հասանելիություն ունենալու իրավունքի երկրորդ բաղադրիչ)։ Այն նույնպես կիրառելի է, և այլ անձանց իրավունքներն ու ազատությունները հաշվի են առնվում, երբ անձնական տվյալներին հասանելիությունը բացառապես ապահովվում է կրկնօրինակը տրամադրելուց բացի այլ միջոցներով։ Օրինակ, հիմնավորված չէ այն տարբերությունը, որ առևտրային գաղտնիքները շոշափում են կրկնօրինակը տրամադրելու կամ տվյալների սուբյեկտին տեղում հասանելիություն ապահովելու միջոցով։ Ինչպես նշված է ՏՊԸԿ 15(1)«ա»-«ը» հոդվածով, ՏՊԸԿ 15(4) հոդվածը կիրառելի չէ մշակման վերաբերյալ լրացուցիչ տեղեկությունների նկատմամբ։

170. 63-րդ ներածական դրույթի համաձայն՝ հակադիր իրավունքներն ու ազատությունները ներառում են առևտրային գաղտնիքները կամ մտավոր սեփականությունը և, մասնավորապես, այն հեղինակային իրավունքը, որով պաշտպանված են ծրագրային ապահովումները։ Բացահայտ կերպով նշված այս իրավունքներն ու ազատությունները պետք է դիտարկվեն զուտ որպես օրինակներ, քանի որ, սկզբունքորեն, Միության կամ անդամ պետության իրավունքի վրա հիմնված ցանկացած իրավունք կամ ազատություն կարող է հիմք ծառայել ՏՊԸԿ 15(4) հոդվածի սահմանափակման համար[96]։ Այսպիսով, անձնական տվյալների պաշտպանության իրավունքը (Հիմնարար իրավունքների եվրոպական խարտիայի 8-րդ հոդված) ՏՊԸԿ 15(4) հոդվածի իմաստով նույնպես կարող է համարվել շոշափված իրավունք։ Ինչ վերաբերում է կրկնօրինակը ձեռք բերելու իրավունքին՝ այլ անձանց տվյալների պաշտպանության իրավունքն այն տիպիկ դեպքն է, երբ սահմանափակումը պետք է գնահատվի։ Ավելին, նամակագրության, օրինակ՝ աշխատավայրում մասնավոր էլեկտրոնային նամակագրության գաղտնիության իրավունքը պետք է հաշվի առնվի[97]։ Կարևոր է նշել, որ ոչ բոլոր շահերն են համարվում «իրավունքներ և ազատություններ»՝ համաձայն ՏՊԸԿ 15(4) հոդվածի։ Օրինակ՝ անձնական տվյալները չհրապարակելու՝ ընկերության տնտեսական շահերը չեն բավարարում 15(4) հոդվածով նախատեսված բացառություն կիրառելու շեմը, քանի դեռ չեն շոշափվում առևտրային գաղտնիքները, մտավոր սեփականությունը կամ այլ պաշտպանված իրավունքները։

171. «Այլ անձինք» եզրույթը նշանակում է տվյալների սուբյեկտից բացի ցանկացած այլ ֆիզիկական կամ իրավաբանական անձ, որն իրացնում է իր հասանելիություն ունենալու իրավունքը։ Հետևաբար, կարող են դիտարկվել հսկողի կամ մշակողի (օրինակ՝ առևտրային գաղտնիքները և մտավոր սեփականությունը գաղտնի պահելու առնչությամբ) իրավունքներն ու ազատությունները։ Եթե ԵՄ օրենսդիրը ցանկանար բացառել հսկողների կամ մշակողների իրավունքներն ու ազատությունները, ապա կօգտագործեր «երրորդ անձ» եզրույթը, որը սահմանված է ՏՊԸԿ 4(10) հոդվածում։

---

[96] Հակադիր իրավունքների ու ազատությունների կշիռը կամ առաջնահերթությունը «իրավունքներ ու ազատություններ» եզրույթների սահմանման հարցը չէ։ Այնուամենայնիվ, այդ շահերի հակակշռումը գնահատման երկրորդ քայլի մի մասն է՝ արդյոք 15(4) հոդվածը կիրառելի է, թե ոչ։ Տե՛ս ստորև ներկայացված 173-րդ պարբերությունը։

[97] ՄԻԵԿ, Բարբուլեսկուն *ընդդեմ Ռումինիայի գործ* [Bărbulescu v. Romania], Գանգատ թիվ 61496/08, պաբերություն 80, 2017 թվականի սեպտեմբերի 5։

172. Այն ընդհանուր մտահոգությունը, որ այլ անձանց իրավունքներն ու ազատությունները կարող են շոշափվել հասանելիություն ստանալու մասին դիմումը բավարարելու արդյունքում, բավարար չէ՝ ՏՊԸԿ 15(4) հոդվածին հղում կատարելու համար: Հսկողը պետք է կարողանա ապացուցել, որ կոնկրետ իրավիճակում այլ անձանց իրավունքները կամ ազատությունները, փաստացիորեն, շոշափված են:

Օրինակ 34. Ներկայումս չափահաս անձի խնամքը մի քանի տարի շարունակ իրականացվել է Երիտասարդների սոցիալական ապահովության գրասենյակ կողմից: Համապատասխան գործի նյութերը կարող են այլ անձանց (ծնողներ, սոցիալական աշխատողներ, այլ անչափահասներ) վերաբերյալ պարունակել գաղտնի տեղեկություններ: Այնուամենայնիվ, տվյալների սուբյեկտի կողմից տեղեկություններ ստանալու մասին դիմումը, որպես կանոն, չի կարող մերժվել այս պատճառով՝ հղում կատարելով ՏՊԸԿ 15(4) հոդվածին: Ավելի շուտ, այլ անձանց իրավունքներն ու ազատությունները պետք է մանրամասնորեն ուսումնասիրվեն և ներկայացվեն Երիտասարդների սոցիալական ապահովության գրասենյակ կողմից՝ որպես հսկող: Ելնելով խնդրո առարկա շահերից և դրանց հարաբերական կշռից՝ այդպիսի կոնկրետ տեղեկությունների տրամադրումը կարող է մերժվել (օրինակ՝ խմբագրելով անունները):

173. Ինչ վերաբերում է ՏՊԸԿ 4-րդ ներածական դրույթին և Հիմնարար իրավունքների եվրոպական խարտիայի 52(1) հոդվածի հիմքում ընկած հիմնավորմանը՝ անձնական տվյալների պաշտպանության իրավունքը բացարձակ իրավունք չէ[98]: Հետևաբար, հասանելիություն ունենալու իրավունքի իրացումը պետք է հակակշռվի այլ հիմնարար իրավունքների հետ՝ համաչափության սկզբունքին համապատասխան: Երբ ՏՊԸԿ 15(4) հոդվածի գնահատմամբ ապացուցվում է, որ դիմումի բավարարումը հակառակ (բացասական) ազդեցություն ունի այլ մասնակիցների իրավունքների ու ազատությունների վրա (քայլ 1), բոլոր մասնակիցների շահերը պետք է կշռվեն՝ հաշվի առնելով գործի հատուկ հանգամանքները և մասնավորապես՝ տվյալների փոխանցման ժամանակ առկա ռիսկերի հավանականությունն ու լրջությունը: Հսկողը պետք է փորձի համատեղել հակադիր իրավունքները (քայլ 2), օրինակ՝ այլ անձանց իրավունքների ու ազատությունների ռիսկը մեղմացնող համապատասխան միջոցների իրականացման միջոցով: Ինչպես ընդգծվում է 63-րդ ներածական դրույթի մեջ, այլ անձանց իրավունքների ու ազատությունների պաշտպանությունը ՏՊԸԿ 15(4) հոդվածի ուժով չպետք է հանգեցնի տվյալների սուբյեկտին բոլոր տեղեկությունները տրամադրելու մերժմանը: Սա նշանակում է, օրինակ, որ երբ սահմանափակումը կիրառվում է, այլ անձանց վերաբերող տեղեկությունները պետք է հնարավորինս անընթեռնելի դարձվեն՝ անձնական տվյալների կրկնօրինակը տրամադրելուց հրաժարվելու փոխարեն: Այնուամենայնիվ, եթե հնարավոր չէ գտնել լուծում համապատասխան իրավունքների համատեղման առումով, ապա հսկողը հաջորդ քայլով պետք է որոշի, թե հակադիր իրավունքներից և ազատություններից որն է գերակայում (քայլ 3):

[98] Տե՛ս նաև ԵՄԱԴ, թիվ C-92/09 և թիվ C-93/09 միացված գործեր, *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen* [ՄՊ], 2010 թվականի նոյեմբերի 9, պարբերություն 48:

Օրինակ 35. Մանրածախ առևտրով զբաղվող վաճառողն իր հաճախորդներին հնարավորություն է տալիս արտադրանք պատվիրել իր հաճախորդների սպասարկման ծառայության թեժ գծի միջոցով: Առևտրային գործարքներն ապացուցելու նպատակով մանրածախ առևտրով զբաղվող վաճառողը պահպանում է զանգերի ձայնագրությունը՝ կիրառելի օրենսդրության խիստ պահանջներին համապատասխան: Հաճախորդը ցանկանում է ստանալ հաճախորդների սպասարկման ծառայության ներկայացուցչի հետ ունեցած զրույցի կրկնօրինակը: Առաջին քայլով մանրածախ առևտրով զբաղվող վաճառողը վերլուծում է դիմումը և հասկանում, որ ձայնագրությունը պարունակում է նաև մեկ այլ անձին, մասնավորապես՝ հաճախորդների սպասարկման ծառայության ներկայացուցչին վերաբերող անձնական տվյալներ: Երկրորդ քայլով, գնահատելու համար, թե արդյոք կրկնօրինակի տրամադրումը կշոշափի այլ անձանց իրավունքներն ու ազատությունները, մանրածախ առևտրով զբաղվող վաճառողը պետք է հակակշռի հակադիր շահերը, հատկապես հաշվի առնելով հաճախորդների սպասարկման ծառայության ներկայացուցչի իրավունքների ու ազատությունների հնարավոր ռիսկերի հավանականությունն ու լրջությունը, որոնք առկա են հաճախորդի հետ հաղորդակցության ձայնագրության մեջ: Մանրածախ առևտրով զբաղվող վաճառողը եզրակացնում է, որ ձայնագրության մեջ առկա են հաճախորդների սպասարկման ծառայության ներկայացուցչին վերաբերող շատ սահմանափակ թվով անձնական տվյալներ, միայն նրա ձայնը: Մանրածախ առևտրով զբաղվող վաճառողը/հսկողը գտնում է, որ ներկայացուցիչը հեշտությամբ չի նույնականացվում: Ընդ որում, քննարկումը կրում է մասնագիտական բնույթ, իսկ զրուցակիցը տվյալների սուբյեկտն է: Վերոհիշյալ հանգամանքների հիման վրա հսկողն օբյեկտիվորեն եզրակացնում է, որ հասանելիություն ունենալու իրավունքը բացասաբար չի անդրադառնում հաճախորդների սպասարկման ծառայության ներկայացուցչի իրավունքների ու ազատությունների վրա, և, հետևաբար, հսկողը կարող է տվյալների սուբյեկտին տրամադրել ամբողջական ձայնագրությունը, այդ թվում՝ ձայնային ձայնագրության այն մասերը, որոնք վերաբերում են հաճախորդների սպասարկման ծառայության ներկայացուցչին:

Օրինակ 36. Բժշկական պարագաների խանութի հաճախորդը ցանկանում է հասանելիություն ստանալ իր ոտքերի չափման արդյունքներին ՏՊԸԿ 15-րդ հոդվածի հիման վրա: Բժշկական պարագաների խանութը չափել է տվյալների սուբյեկտի ոտքերը՝ անհատական բժշկական կոմպրեսիոն գուլպաներ պատրաստելու համար: Ենթադրաբար, բժշկական պարագաների խանութը մեծ փորձառություն ուներ և ներդրել էր ճշգրիտ չափումների հատուկ տեխնիկա: Բժշկական պարագաների խանութում չափելուց հետո հաճախորդը ցանկանում է օգտագործել չափման արդյունքները՝ գուլպաները մեկ այլ խանութից ավելի էժան գնելու համար (պատվիրելով դրանք առցանց խանութում): Բժշկական պարագաների խանութը մասամբ մերժում է տվյալներին հասանելիությունը ՏՊԸԿ 15(4) հոդվածի հիման վրա՝ պնդելով, որ իրենց հատուկ, ճշգրիտ չափման տեխնիկայի շնորհիվ արդյունքները պաշտպանված են՝ որպես առևտրային գաղտնիք: Եթե, այնքանով, որքանով հսկողը կարող է ապացուցել, որ.

- տվյալների սուբյեկտին չափման արդյունքների վերաբերյալ տեղեկություններ տրամադրելը հնարավոր չէ առանց չափումների կատարման եղանակը բացահայտելու և
- չափումների կատարման եղանակի վերաբերյալ տեղեկությունները, այդ թվում, հարկ եղած դեպքում, չափման կետերի ճշգրիտ որոշումը հանդիսանում են առևտրային գաղտնիք, ապա

նա կարող է կիրառել ՏՊԸԿ 15(4) հոդվածը:

Այնուամենայնիվ, հսկողը պետք է տրամադրի չափումների արդյունքների վերաբերյալ հնարավորինս շատ տեղեկություններ, որոնք չեն բացահայտի իր առևտրային գաղտնիքը, նույնիսկ եթե դա ենթադրի արդյունքները վերանայելու և խմբագրելու ջանքեր:

Օրինակ 37. Χ ԽԱՂԱՑՈՂԸ գրանցված է Υ ՀԱՐԹԱԿԻ խաղային հարթակում՝ որպես օգտատեր: Մի օր Χ ԽԱՂԱՑՈՂԸ ծանուցվում է, որ իր առցանց հաշիվը սահմանափակվել է: Քանի որ նա այլևս չի կարողանում մուտք գործել իր հաշիվ, Χ ԽԱՂԱՑՈՂԸ դիմում է հսկողին խնդրանքով տրամադրել իրեն վերաբերող բոլոր անձնական տվյալներին հասանելիություն: Բացի դրանից, Χ ԽԱՂԱՑՈՂԸ պահանջում է իրեն ներկայացնել հաշվի սահմանափակման պատճառները: Υ ՀԱՐԹԱԿԸ՝ առցանց խաղային հարթակի հսկողը, որին ներկայացվել է դիմումը, օգտատերերին իր կայքում հրապարակված ընդհանուր պայմաններով տեղեկացնում է, որ ցանկացած տեսակի խաբեություն (հիմնականում երրորդ անձի ծրագրային ապահովում կիրառելու միջոցով) կհանգեցնի իր հարթակից ժամանակավոր կամ մշտական հեռացման: Υ ՀԱՐԹԱԿՆ իր գաղտնիության քաղաքականության մեջ նույնպես տեղեկացնում է օգտատերերին անձնական տվյալների մշակման մասին՝ խաղային խաբեությունների հայտնաբերման նպատակով՝ ՏՊԸԿ 13-րդ հոդվածով սահմանված պահանջներին համապատասխան:

Χ ԽԱՂԱՑՈՂԻ՝ հասանելիություն ստանալու մասին դիմումն ստանալուց հետո Υ ՀԱՐԹԱԿԸ պետք է Χ ԽԱՂԱՑՈՂԻՆ տրամադրի նրա վերաբերյալ մշակված անձնական տվյալների կրկնօրինակը: Հաշվի սահմանափակման պատճառների առնչությամբ Υ ՀԱՐԹԱԿԸ պետք է հաստատի Χ ԽԱՂԱՑՈՂԻՆ, որ որոշել է սահմանափակել նրա առցանց խաղերին հասանելիությունը՝ մեկ կամ ավելի խաղային խաբեություններ կատարելու պատճառով, որոնք խախտում են օգտագործման ընդհանուր պայմանները: Ի հավելումն խաղային խաբեությունների հայտնաբերման նպատակով մշակման վերաբերյալ տրամադրված տեղեկությունների, Υ ՀԱՐԹԱԿԸ պետք է Χ ԽԱՂԱՑՈՂԻՆ հասանելիություն տրամադրի Χ ԽԱՂԱՑՈՂԻ խաղային խաբեությունների մասին իր պահած տեղեկություններին, որը հանգեցրել է սահմանափակմանը: Մասնավորապես, Υ ՀԱՐԹԱԿԸ պետք է Χ ԽԱՂԱՑՈՂԻՆ տրամադրի այն տեղեկությունները, որոնք հանգեցրել են հաշվի սահմանափակմանը (օրինակ՝ մատյանների ամփոփագիրը, խաբեության ամսաթիվը և ժամը, երրորդ կողմի ծրագրային ապահովման հայտնաբերումը…), որպեսզի տվյալների սուբյեկտը (այսինքն՝ Χ ԽԱՂԱՑՈՂԸ) ստուգի, որ տվյալների մշակումը ճիշտ է իրականացվել:

Այնուամենայնիվ, ՏՊԸԿ 15(4) հոդվածի և ՏՊԸԿ 63-րդ ներածական դրույթի համաձայն՝ Υ ՀԱՐԹԱԿԸ պարտավոր չէ բացահայտել խաբեությունների դեմ պայքարի ծրագրային ապահովման տեխնիկական աշխատանքի որևէ մասը, նույնիսկ եթե այդ տեղեկությունները վերաբերում են Χ ԽԱՂԱՑՈՂԻՆ, քանի որ դրանք կարող են համարվել առևտրային գաղտնիք: ՏՊԸԿ 15(4) հոդվածի համաձայն՝ շահերի անհրաժեշտ հակակշռումը կհանգեցնի նրան, որ Υ ՀԱՐԹԱԿԻ առևտրային գաղտնիքների պատճառով կբացառվի այդ անձնական տվյալների հրապարակումը, քանի որ խաբեությունների դեմ պայքարի ծրագրային ապահովման տեխնիկական աշխատանքի մասին իմացությունը կարող է նաև թույլ տալ օգտատիրոջը շրջանցել ապագա խաբեության կամ խարդախության հայտնաբերումը[99]:

174. Եթե հսկողները հրաժարվում են բավարարել ՏՊԸԿ 15(4) հոդվածի համաձայն հասանելիություն ունենալու իրավունքի իրացման մասին դիմումն ամբողջությամբ կամ մասամբ, ապա նրանք պետք է անհապաղ և ամենաուշը մեկ ամսվա ընթացքում տեղեկացնեն տվյալների սուբյեկտին դրա պատճառների մասին (ՏՊԸԿ 12(4) հոդված): Բացատրության մեջ պետք է նշվեն կոնկրետ հանգամանքները, որպեսզի տվյալների սուբյեկտները կարողանան գնահատել, թե արդյոք ցանկանում են մերժման առնչությամբ քայլեր ձեռնարկել, թե ոչ: Այն պետք է տեղեկություններ պարունակի վերահսկող մարմին բողոք ներկայացնելու (ՏՊԸԿ 77-րդ հոդված) և դատական պաշտպանության միջոցներ հայցելու հնարավորության մասին (ՏՊԸԿ 79-րդ հոդված):

6.3 ՏՊԸԿ 12(5) հոդվածը

175. ՏՊԸԿ 12(5) հոդվածը հնարավորություն է տալիս հսկողներին չբավարարել հասանելիություն ունենալու իրավունքի իրացման մասին այն դիմումները, որոնք ակնհայտորեն անհիմն կամ սահմանազանցող են: Այս հասկացություններին պետք է տալ նեղ մեկնաբանություն, քանի որ թափանցիկության և տվյալների սուբյեկտների իրավունքների անվճար իրացման սկզբունքները չպետք է խաթարվեն:

176. Հսկողները պետք է կարողանան ապացուցել անձին, թե ինչու են նրանք կարծում, որ դիմումն ակնհայտորեն անհիմն կամ սահմանազանցող է, և հարց առաջանալու դեպքում բացատրել դրա պատճառներն իրավասու վերահսկող մարմնին: Յուրաքանչյուր դիմում պետք է դիտարկվի ըստ յուրաքանչյուր կոնկրետ դեպքի՝ որոշելու համար, թե արդյոք այն ակնհայտորեն անհիմն կամ սահմանազանցող է, թե ոչ:

6.3.1 Ի՞նչ է նշանակում ակնհայտորեն անհիմն

177. Հասանելիություն ունենալու իրավունքի իրացման մասին դիմումն ակնհայտորեն անհիմն է, եթե օբյեկտիվ մոտեցում կիրառելիս ՏՊԸԿ 15-րդ հոդվածի պահանջները հստակորեն և ակնհայտորեն պահպանված չեն: Այնուամենայնիվ, ինչպես ներկայացված է հատկապես վերոնշյալ 3-րդ բաժնում, հասանելիություն ունենալու իրավունքի իրացման մասին դիմումների բավարարման շատ քիչ նախապայմաններ կան: Հետևաբար, ՏՊԵԽ-ն ընդգծում է, որ շատ սահմանափակ դեպքերում է հնարավոր հողում կատարել ՏՊԸԿ 12(5) հոդվածով նախատեսված՝ հասանելիություն ունենալու իրավունքի իրացման մասին դիմումների «ակնհայտորեն անհիմն» լինելուն:

[99] Անձանց տրամադրվող տեղեկությունների ծավալը մեծապես կախված կլինի համատեքստից՝ հաշվի առնելով հսկողի բնույթը և սպասարկման պայմանների խախտման բնույթը: Որոշ դեպքերում հսկողը կարող է տրամադրել միայն հիմնական տեղեկություններ՝ ի պատասխան հասանելիություն ստանալու մասին այն դիմումին, որի նկատմամբ կիրառվում է 15(4) հոդվածը:

178. Ավելին, կարևոր է հիշել, որ մինչև սահմանափակումը վկայակոչելը, հսկողները պետք է մանրամասնորեն վերլուծեն դիմումի բովանդակությունն ու շրջանակը: Օրինակ՝ դիմումը չպետք է ակնհայտորեն անհիմն համարվի, եթե այն կապված է ՏՊԸԿ գործողության շրջանակներում չներառվող անձնական տվյալների մշակման հետ (այս դեպքում դիմումին չպետք է ընթացք տրվի որպես 15-րդ հոդվածի գործողությամբ կարգավորվող դիմում):

179. Մյուս դեպքերում ներկայացվող դիմումները, որոնց պարագայում ՏՊԸԿ 12(5) հոդվածի կիրառելիությունը վիճարկելի է, այն տեղեկություններին կամ մշակման գործողություններին վերաբերող դիմումներն են, որոնք հստակորեն և ակնհայտորեն ենթակա չեն հսկողի կողմից մշակման:

> **Օրինակ 38.** Տվյալների սուբյեկտը դիմում է ներկայացնում քաղաքային իշխանություններին այն տվյալներին հասանելիություն ստանալու մասին, որոնք մշակվում են պետական մարմնի կողմից: Դիմումի ակնհայտորեն անհիմն լինելն ապացուցելու փոխարեն առավել հարմար և հեշտ կլինի, եթե մարմինը, որին դիմումը ներկայացված է, հաստատի, որ այդ տվյալները չեն մշակվում այդ մարմնի կողմից (ՏՊԸԿ 15-րդ հոդվածի առաջին բաղադրիչ. «արդյոք» անձնական տվյալները մշակվում են)[100]:

180. Հսկողը չպետք է ենթադրի, որ դիմումն ակնհայտորեն անհիմն է, քանի որ տվյալների սուբյեկտը նախկինում ներկայացրել է ակնհայտորեն անհիմն կամ սահմանազանցող դիմումներ, կամ եթե դրանք պարունակում են ոչ օբյեկտիվ կամ ոչ պատշաճ ձևակերպումներ:

6.3.2 Ի՞նչ է նշանակում սահմանազանցող

181. ՏՊԸԿ-ով չի տրվում «սահմանազանցող» եզրույթի սահմանումը: Մի կողմից ՏՊԸԿ 12(5) հոդվածի «հատկապես դրանց կրկնվող բնույթի պատճառով» ձևակերպումը թույլ է տալիս եզրակացնել, որ ՏՊԸԿ 15-րդ հոդվածի առնչությամբ այս հայեցակետի կիրառման հիմնական պատճառը կապված է տվյալների սուբյեկտի՝ հասանելիություն ունենալու իրավունք ստանալու մասին դիմումների քանակի հետ: Մյուս կողմից, վերը նշված արտահայտությունը ցույց է տալիս, որ մյուս պատճառները, որոնք կարող են հանգեցնել սահմանազանցության, *ի սկզբանե* չեն բացառվում:

182. Անշուշտ, կրկնօրինակը ձեռք բերելու իրավունքի վերաբերյալ ՏՊԸԿ 15(3) հոդվածի համաձայն՝ տվյալների սուբյեկտը կարող է հսկողին ներկայացնել մեկից ավելի դիմումներ[101]: Այն դիմումների դեպքում, որոնք պոտենցիալ կարող են սահմանազանցող համարվել, «սահմանազանցության» գնահատումը կախված է հսկողի կողմից իրականացվող վերլուծությունից և այն ոլորտի առանձնահատկություններից, որտեղ նա գործունեություն է ծավալում:

183. Հետագա դիմումների դեպքում անհրաժեշտ է գնահատել, թե արդյոք ողջամիտ ժամանակահատվածի շեմը (տե՛ս 63-րդ ներածական դրույթը) գերազանցվել է, թե ոչ: Հսկողները պետք է մանրամասնորեն հաշվի առնեն յուրաքանչյուր դեպքի կոնկրետ հանգամանքները: Մյուս կողմից, նույն տվյալների սուբյեկտի կողմից երկրորդ դիմումը կարող է որոշ դեպքերում կրկնվող համարվել:

---

[100] Այլ հարց է, թե արդյոք այն մարմինը, ում ներկայացված է հասանելիություն ստանալու մասին դիմումը, իրավասու է այն փոխանցել իրավասու պետական մարմին, թե ոչ:

[101] 15(3) հոդվածի երկրորդ նախադասության համաձայն՝ հսկողը կարող է ողջամիտ վճար գանձել պահանջվող լրացուցիչ կրկնօրինակների համար:

184. Օրինակ՝ սոցիալական ցանցերի դեպքում տվյալների հավաքածուի մեջ փոփոխությունները տեղի են ունենում ավելի հաճախ, քան հողային կադաստրներում կամ ընկերությունների կենտրոնական ռեգիստրներում: Բիզնես գործընկերների դեպքում անհրաժեշտ է հաշվի առնել հաճախորդի հետ շփումների հաճախականությունը: Ըստ այդմ, «ողջամիտ ժամանակահատվածը», որի ընթացքում տվյալների սուբյեկտները կարող են կրկին իրացնել իրենց հասանելիություն ունենալու իրավունքը, նույնպես տարբեր են: Որքան հաճախ են հսկողի տվյալների բազայում փոփոխություններ տեղի ունենում, այնքան ավելի հաճախ է թույլ տրվում տվյալների սուբյեկտներին դիմել իրենց անձնական տվյալներին հասանելիություն ստանալու համար՝ առանց այն սահմանազանցող համարելու:

185. Ողջամիտ ժամանակահատվածի լրանալու փաստը որոշելիս հսկողները, տվյալների սուբյեկտի ողջամիտ ակնկալիքների լույսի ներքո, պետք է հաշվի առնեն հետևյալը.

- որքա՞ն հաճախ են տվյալները փոխվում. անհավանակա՞ն է, որ տեղեկությունները փոխվեն դիմումների միջև ընկած ժամանակահատվածում: Եթե տվյալների պահոցը պահպանումից բացի ակնհայտորեն ենթակա չէ մշակման, և տվյալների սուբյեկտը տեղյակ է դրա մասին, օրինակ՝ հասանելիություն ունենալու իրավունքի մասին նախկին դիմումից, ապա այդ հանգամանքը կարող է վկայել դիմումի սահմանազանցող լինելու մասին.
- տվյալների բնույթը. այսինքն՝ արդյո՞ք դրանք հանդիսանում են հույժ գաղտնի.
- մշակման նպատակները. այսինքն՝ արդյո՞ք հրապարակվելու դեպքում մշակումը կարող է վնաս հասցնել դիմողին.
- արդյո՞ք հաջորդող դիմումները վերաբերում են միևնույն տեղեկություններին կամ մշակման գործողություններին, թե այլ հարցերի[102]:

Օրինակ 39 (ատաղձագործ). Տվյալների սուբյեկտը **յուրաքանչյուր երկու ամիսը** մեկ հասանելիություն ստանալու մասին դիմումներ է ներկայացնում իր համար սեղան պատրաստած ատաղձագործին: Ատաղձագործն ամբողջությամբ պատասխանել է առաջին դիմումին: Ողջամիտ ժամանակահատվածի լրանալու փաստը որոշելիս պետք է հաշվի առնել, որ ատաղձագործը միայն երբեմն (վերևի առաջին կետ) և ոչ որպես իր հիմնական գործունեության մաս է մշակում և հավաքում անձնական տվյալներ, և նույնիսկ քիչ է հավանականությունը, որ ատաղձագործը հաճախ ծառայություններ մատուցի նույն տվյալների սուբյեկտին: Իսկապես, տվյալ դեպքում ատաղձագործը միայն մեկ անգամ է ծառայություններ մատուցել տվյալների սուբյեկտին, ինչը քչացնում է հավանականությունը, որ տվյալների սուբյեկտին վերաբերող տվյալների հավաքածուի մեջ փոփոխություններ տեղի ունեցած լինեն: Հատկանշական է, որ հաշվի առնելով մշակված անձնական տվյալների բնույթը և ծավալը, մշակման հետ կապված ռիսկերը կարող են ցածր համարվել (վերևի երկրորդ կետ), օրինակ՝ մշակման նպատակը (հաշիվներ ներկայացնելու նպատակները և հաշվառում իրականացնելու պարտավորության կատարումը) չի կարող վնաս հասցնել տվյալների սուբյեկտին (վերևի երրորդ կետ): Բացի դրանից, դիմումը վերաբերում է նույն տեղեկություններին, ինչ վերջին դիմումը (վերևի չորրորդ կետ): Այդ դիմումները, որպես հետևանք, կարող են համարվել սահմանազանցող՝ իրենց կրկնվելու պատճառով:

Օրինակ 40 (սոցիալական մեդիա հարթակ). Սոցիալական մեդիա հարթակը, որի հիմնական գործունեությունը տվյալների սուբյեկտի անձնական տվյալների հավաքումը և (կամ) մշակումն է, իրականացնում է լայնամասշտաբ համապարփակ և շարունակական մշակման գործողություններ: Տվյալների սուբյեկտը, որն օգտվում է հարթակի ծառայություններից, հասանելիություն ստանալու մասին դիմումներ է ներկայացնում **յուրաքանչյուր երեք ամիսը մեկ**: Այս դեպքում մեծ է հավանականությունը, որ տվյալների սուբյեկտին վերաբերող անձնական տվյալները հաճախակի կփոփոխվեն (վերևի առաջին կետ), հավաքագրված տվյալների լայն շրջանակը ներառում է դուրս բերված գաղտնի անձնական տվյալները (վերևի երկրորդ կետ), որոնք մշակվել են՝ տվյալների սուբյեկտին համապատասխան կոնտենտ և ցանցի անդամներին ցույց տալու նպատակով (երրորդ կետ): Հասանելիություն ստանալու մասին դիմումները յուրաքանչյուր երեք ամիսը մեկ կարող են, այս հանգամանքներում, սկզբունքորեն չհամարվել որպես սահմանազանցող՝ կրկնվելու պատճառով:

[102] Եթե հետագա դիմումը վերաբերում է ծավալով ԵՎ ժամանակով միևնույն տեղեկություններին, ապա սա ոչ թե սահմանազանցության, այլ լրացուցիչ կրկնօրինակ ստանալու խնդրանքի հարց է, տե՛ս 2.2.2.2 բաժինը:

Օրինակ 41 (վարկային գործակալություններ). Ինչպես սոցիալական ցանցերում, այնպես էլ վարկային գործակալությունների դեպքում չի կարելի բացառել, որ վերջիններիս տիրապետման տակ գտնվող համապատասխան տվյալները կփոփոխվեն շատ ավելի հաճախ, քան այլ ոլորտներում (վերևի առաջին կետ): Սա պայմանավորված է բազմաթիվ գործոններով, որոնց մասին տվյալների սուբյեկտը, որպես ներքին տեղեկությունների չտիրապետող անձ, սովորաբար տեղյակ չէ բիզնես մոդելի բարդության պատճառով: Այն հարցի պատասխանը, թե ինչ տեսակի տվյալներ է հավաքել հսկողը բալային արժեքի հաշվարկման համար, և որոնք են ներկայումս ներառված հաշվարկում, կարող է տալ միայն վարկային գործակալությունը: Բացի դրանից, վարկային գործակալությունների միջոցով տվյալների մշակումը և արդյունքում ստացված բալային արժեքը կարող է խոր հետևանքներ ունենալ տվյալների սուբյեկտի համար՝ կապված ենթադրյալ իրավական գործարքների, ինչպիսիք են գնման, վարձակալության կամ լիզինգի պայմանագրերի կնքման հետ (վերևի երրորդ կետ):
Ընդհանուր առմամբ հնարավոր չէ որոշել որևէ կոնկրետ ժամանակահատված, որի ընթացքում հասանելիություն ստանալու մասին հետագա դիմում ներկայացնելը կարող է սահմանազանցող համարվել՝ ՏՊԸԿ 12(5) հոդվածի երկրորդ նախադասության համաձայն: Ավելի շուտ անհրաժեշտ է ընդհանուր կերպով դիտարկել առանձին գործի հանգամանքները: Այնուամենայնիվ, հաշվի առնելով տվյալների մշակման կարևորությունը տվյալների սուբյեկտների առօրյա կյանքի համար, կարելի է ենթադրել, որ անվճար տրամադրվող տեղեկությունների միջև մեկ տարվա ժամանակահատվածն ամեն դեպքում չափազանց մեծ կլինի, որպեսզի դիմումը սահմանազանցող համարվի: Եթե դիմումը ներկայացվում է շատ կարճ ժամանակահատվածի ընթացքում, ապա որոշիչ գործոնը պետք է լինի այն, թե արդյոք տվյալների սուբյեկտը հիմքեր ունի ենթադրելու, որ տեղեկությունները կամ մշակումը փոխվել է վերջին դիմումից հետո: Օրինակ, եթե տվյալների սուբյեկտն իրականացրել է ֆինանսական գործարք, օրինակ՝ վարկ է վերցնել, ապա տվյալների սուբյեկտը պետք է իրավունք ունենա դիմելու վարկային տեղեկություններին հասանելիություն ստանալու խնդրանքով, թեև այդ դիմումը ներկայացվել և դրա պատասխանը տրվել է կարճ ժամանակ առաջ:

186. Երբ հնարավոր է լինում տեղեկությունները հեշտությամբ տրամադրել էլեկտրոնային միջոցներով կամ անվտանգ համակարգին հեռավար հասանելիություն ապահովելու միջոցով, ինչը նշանակում է, որ այդ դիմումների բավարարումը ծանրաբեռնվածություն չի առաջացնում հսկողի համար, քիչ հավանական է, որ հետագա դիմումները կարող են սահմանազանցող համարվել:

187. Եթե դիմումը համընկնում է նախորդ դիմումի հետ, ապա այն կարող է ընդհանուր առմամբ սահմանազանցող համարվել, երբ և եթե պարունակում է նույն տեղեկությունները կամ մշակման գործողությունները, և հսկողը դեռևս չի բավարարել նախորդ դիմումը՝ առանց «անհիմն ձգձգման» վիճակի շեմն անցնելու (տե՛ս ՏՊԸԿ 12(3) հոդված): Գործնականում, երկու դիմումներն արդյունքում կարող են միացվել:

188. Այն փաստը, որ հսկողից հսկայական ջանք ու ժամանակ է պահանջվելու տեղեկությունները կամ կրկնօրինակը տվյալների սուբյեկտին տրամադրելու համար, չի կարող ինքնին դիմումը դարձնել սահմանազանցող[103]: Հասանելիություն ստանալու մասին դիմումները բավարարելիս մեծ թվով մշակման գործողությունները սովորաբար պահանջում են առավել մեծ ջանքեր: Այնուամենայնիվ, ինչպես վերը նշվեց, որոշ դեպքերում դիմումները կարող են սահմանազանցող համարվել իրենց կրկնվող բնույթից բացի այլ պատճառներով: Ըստ ՏՊԵԽ-ի՝ սա մասնավորապես ներառում է ՏՊԸԿ 15-րդ հոդվածին չափից շատ հղում կատարելու դեպքերը, որի պարագայում տվյալների սուբյեկտները չարաշահում են հասանելիություն ունենալու իրավունքի իրացումը՝ հսկողին վնաս պատճառելու միակ մտադրությամբ:

[103] Համաչափության սկզբունքի ստուգում չի իրականացվել, տե՛ս վերևի 166-րդ պարբերությունը:

189. Այս իրավիճակում դիմումը չպետք է սահմանազանցող համարվի այն հիմքով, որ.

- տվյալների սուբյեկտը դիմումի առնչությամբ որևէ պատճառ չի նշում, կամ հսկողը դիմումը համարում է անիմաստ.
- տվյալների սուբյեկտը կիրառում է ոչ պատշաճ կամ անքաղաքավարի ձևակերպում.
- տվյալների սուբյեկտը մտադիր է տվյալներն օգտագործել հսկողի դեմ հետագայում հայց ներկայացնելու համար:[104]

190. Մյուս կողմից, դիմումը կարող է սահմանազանցող համարվել, օրինակ, եթե.

- անձը դիմում է ներկայացնում, սակայն միևնույն ժամանակ առաջարկում է չեղարկել այն՝ հսկողից որոշ օգուտ ստանալու դիմաց, կամ
- դիմումը ներկայացվել է չարամտորեն և օգտագործվում է հսկողի կամ նրա աշխատողների նկատմամբ ճնշում գործադրելու համար՝ նպատակ ունենալով միայն խաթարել նրանց աշխատանքը, օրինակ՝ այն փաստի ուժով, որ.
    - անձն իր դիմումի մեջ կամ այլ հաղորդակցություններում բացահայտ կերպով նշել է, որ իր մտադրությունը նրանց աշխատանքը խաթարելն է և ոչ մի այլ նպատակ նա չի հետապնդում, կամ
    - անձն արշավի շրջանակներում պարբերաբար տարբեր դիմումներ է ուղարկում հսկողին, օրինակ՝ շաբաթը մեկ անգամ՝ աշխատանքը խաթարելու մտադրությամբ և նպատակով[105]:

[104] Սա չի հակասում ցանկացած կիրառելի ազգային իրավունքին, որը համապատասխանում է ՏՊԸԿ 23-րդ հոդվածի պահանջներին, տե՛ս 6.4 գլուխը:

[105] «Արշավի շրջանակներում համակարգված ուղարկում» նշանակում է, որ դիմումները, որոնք հեշտությամբ կարող են միավորվել մեկ դիմումի մեջ, արհեստականորեն տվյալների սուբյեկտի կողմից բաժանվում են ոչ միայն մի քանի, այլ շատ առանձին մասերի՝ աշխատանքն ակնհայտորեն խաթարելու մտադրությամբ:

6.3.3 Հետևանքները

191. Հասանելիություն ունենալու իրավունքի իրացման մասին ակնհայտորեն անհիմն կամ սահմանազանցող դիմումի դեպքում հսկողները, ՏՊԸԿ 12(5) հոդվածի համաձայն, կարող են կա՛մ ողջամիտ գումար գանձել (հաշվի առնելով տեղեկությունների կամ հաղորդակցության տրամադրման կամ պահանջվող գործողությունների կատարման վարչական ծախսերը), կա՛մ հրաժարվել դիմումը բավարարելուց:

192. ՏՊԵԽ-ը մատնանշում է, որ մի կողմից հսկողները, որպես կանոն, պարտավոր չեն ողջամիտ գումար գանձել մինչև դիմումը բավարարելուց հրաժարվելը: Մյուս կողմից, նրանք լիովին ազատ չեն ընտրելու երկու այլընտրանքների միջև: Փաստացիորեն, հսկողները պետք է համարժեք որոշում կայացնեն՝ կախված գործի կոնկրետ հանգամանքներից: Թեև դժվար է պատկերացնել, որ ողջամիտ վճար գանձելը հարմար միջոց է ակնհայտորեն անհիմն դիմումների դեպքում, այնուամենայնիվ, սահմանազանցող դիմումների դեպքում, թափանցիկության սկզբունքին համապատասխան, հաճախ ավելի նպատակահարմար կլինի գանձել վճար՝ որպես վարչական ծախսերի փոխհատուցում, որոնք առաջանում են կրկնվող դիմումների դեպքում:

193. Հսկողները պետք է կարողանան ապացուցել դիմումի ակնհայտորեն անհիմն կամ սահմանազանցող բնույթը (ՏՊԸԿ 12(5) հոդվածի երրորդ նախադասություն): Հետևաբար, առաջարկվում է ապահովել դրանց հիմքում ընկած փաստերի պատշաճ փաստաթղթավորումը: ՏՊԸԿ 12(4) հոդվածին համահունչ, եթե հսկողները հրաժարվում են ամբողջությամբ կամ մասամբ բավարարել հասանելիություն ստանալու մասին դիմումը, ապա նրանք պետք է դիմումն ստանալուց հետո անհապաղ և ամենաուշը մեկ ամսվա ընթացքում տեղեկացնեն տվյալների սուբյեկտին.

- պատճառի մասին.
- վերադաս մարմին բողոք ներկայացնելու իրավունքի մասին.
- դատական պաշտպանության միջոց հայցելու հնարավորության մասին:

194. Մինչև ՏՊԸԿ 12(5) հոդվածով նախատեսված ողջամիտ վճարը գանձելը հսկողները պետք է դրա մասին տեղեկացնեն տվյալների սուբյեկտներին: Տվյալների սուբյեկտներին պետք է հնարավորություն տրվի որոշելու, թե արդյոք նրանք կչեղարկեն դիմումը, որպեսզի խուսափեն գումար վճարելուց:

195. Հասանելիություն ունենալու իրավունքի իրացման մասին դիմումների չհիմնավորված մերժումները կարող են համարվել տվյալների սուբյեկտների իրավունքների խախտում՝ ՏՊԸԿ 12-22-րդ հոդվածների համաձայն և, հետևաբար, վերահսկող իրավասու մարմինները կարող են իրականացնել ուղղիչ լիազորություններ, այդ թվում՝ ՏՊԸԿ 83(5)(բ) հոդվածի հիման վրա սահմանել վարչական տուգանքներ: Եթե տվյալների սուբյեկտները կարծում են, որ առկա է իրենց՝ տվյալների սուբյեկտների իրավունքների խախտում, ապա նրանք իրավունք ունեն բողոք ներկայացնելու՝ ՏՊԸԿ 77-րդ հոդվածի հիման վրա:

6.4 ՏՊԸԿ 23-րդ հոդվածի հիման վրա Միության կամ անդամ պետությունների իրավունքով նախատեսված հնարավոր սահմանափակումները և շեղումները

196. ՏՊԸԿ 15-րդ հոդվածով նախատեսված պարտավորությունների և իրավունքների շրջանակը կարող է սահմանափակվել Միության կամ անդամ պետությունների իրավունքով նախատեսված օրենսդրական միջոցներով[106]:

197. Այն հսկողները, որոնք նախատեսում են կիրառել ազգային իրավունքի վրա հիմնված սահմանափակումը, պետք է մանրամասնորեն ստուգեն համապատասխան ազգային օրենսդրության դրույթների պահանջները: Ավելին, կարևոր է նշել, որ անդամ պետությունների (կամ Միության) իրավունքով նախատեսված հասանելիություն ունենալու իրավունքի՝ ՏՊԸԿ 23-րդ հոդվածի վրա հիմնված սահմանափակումներով պետք է խստորեն կատարվեն սույն դրույթով սահմանված պայմանները: ՏՊԵԽ-ը հրապարակել է ՏՊԸԿ 23-րդ հոդվածի համաձայն՝ Սահմանափակումների վերաբերյալ 10/2020 ուղեցույցը՝ դրանց վերաբերյալ լրացուցիչ պարզաբանումներով: Հասանելիություն ունենալու իրավունքի առումով ՏՊԵԽ-ը հիշեցնում է, որ հսկողները պետք է վերացնեն սահմանափակումներն այն պահից, երբ դրանք հիմնավորող հանգամանքներն այլևս առկա չեն[107]:

198. ՏՊԸԿ 23-րդ հոդվածով նախատեսված սահմանափակումներին վերաբերող օրենսդրական միջոցներով կարող է նաև նախատեսվել, որ իրավունքի իրացումը ժամանակի մեջ առկախվում է, որ իրավունքն իրացվում է մասամբ կամ սահմանափակվում է որոշ կատեգորիաների տվյալներով, կամ որ իրավունքը կարող է անուղղակիորեն իրացվել անկախ վերահսկող մարմնի միջոցով[108]:

---

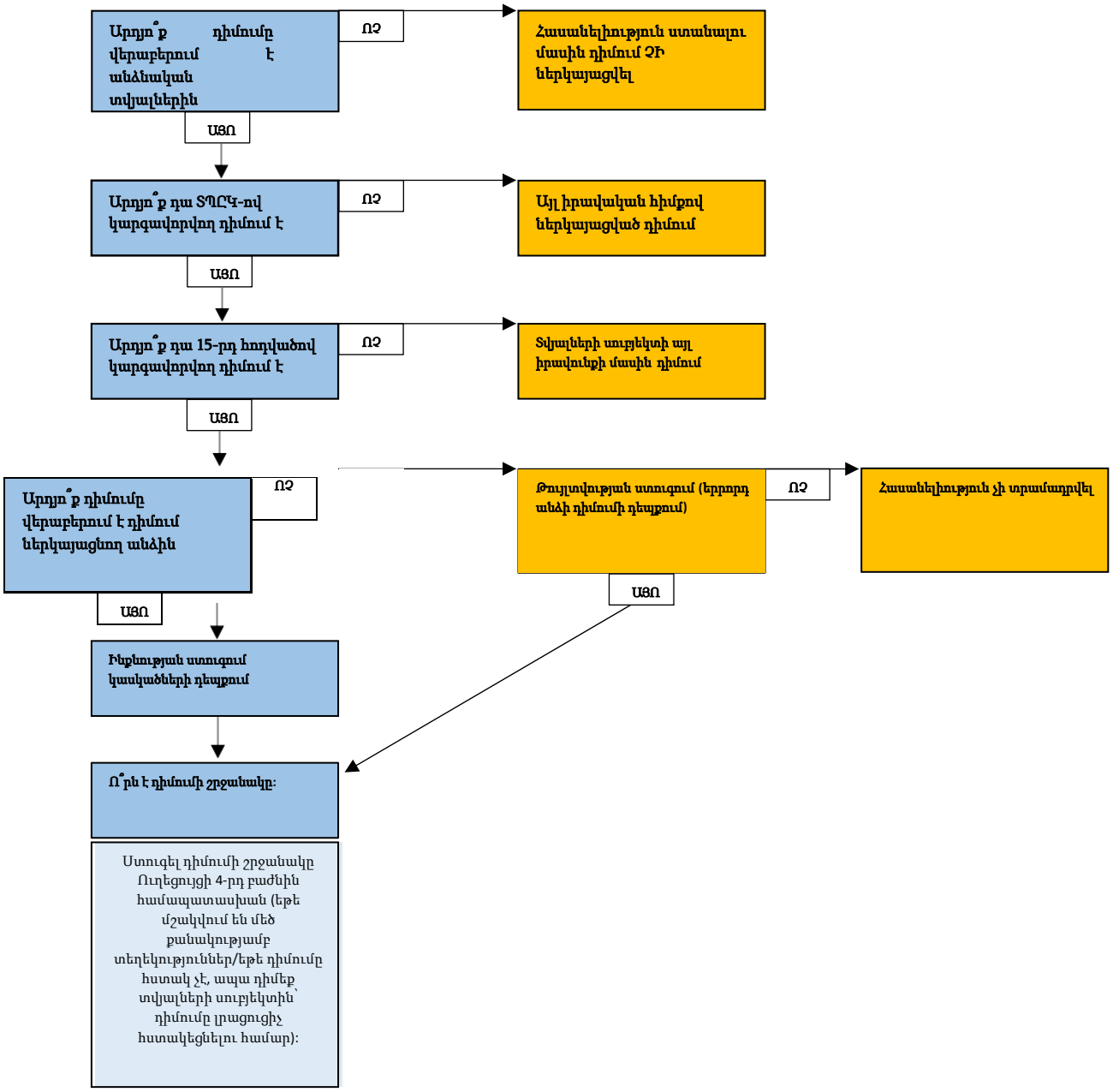
[106] Տե՛ս, օրինակ՝ «Տվյալների պաշտպանության մասին» Գերմանիայի դաշնային ակտի (BDSG) 32-37-րդ հոդվածները, «Անձնական տվյալների պաշտպանության մասին» Նորվեգիայի ակտի 16-րդ և 17-րդ հոդվածները և «Տվյալների պաշտպանության մասին» Շվեդիայի ակտի 5-րդ գլուխը:

[107] ՏՊԸԿ 23-րդ հոդվածի համաձայն՝ Սահմանափակումների վերաբերյալ 10/2020 ուղեցույցի 76-րդ պարբերություն, տարբերակ 2.0, ընդունվել է 2021 թվականի հոկտեմբերի 13-ին:

[108] ՏՊԸԿ 23-րդ հոդվածի համաձայն՝ Սահմանափակումների վերաբերյալ 10/2020 ուղեցույցի 12-րդ պարբերություն, տարբերակ 2.0, ընդունվել է 2021 թվականի հոկտեմբերի 13-ին: «Տվյալների պաշտպանության մասին» Գերմանիայի դաշնային ակտի 34(3) հոդվածով, օրինակ, սահմանվում է, որ եթե պետական մարմինը որոշ սահմանափակումների պատճառով տեղեկություններ չի տրամադրում տվյալների սուբյեկտին հասանելիություն ունենալու իրավունքի իրացման մասին դիմումը բավարարելիս, ապա այդ տեղեկությունները տվյալների սուբյեկտի դիմումի համաձայն տրամադրվում են Դաշնային վերահսկող մարմնին, բացառությամբ այն դեպքերի, երբ պատասխանատու Գերագույն դաշնային մարմինը (մարմինը, ում ներկայացված է դիմումը) առանձին դեպքերում չի որոշում, որ դա կարող է խաթարել Դաշնության կամ երկրի անվտանգությունը: Տվյալների պաշտպանության մասին Իտալիայի օրենսգրքով նախատեսվում է անուղղակի հասանելիություն (մարմնի միջոցով) այն դեպքում, երբ հասանելիությունը կարող է բացասաբար անդրադառնալ մի շարք շահերի (օրինակ՝ փողերի լվացմանը հակադրվող շահի) վրա, տե՛ս Տվյալների պաշտպանության մասին Իտալիայի օրենսգրքի 2-L հոդվածը:

ՀԱՎԵԼՎԱԾ. ԳԾԱՊԱՏԿԵՐ

Քայլ 1. Ինչպե՞ս մեկնաբանել և գնահատել դիմումը



Քայլ 2. Ինչպե՞ս պատասխանել դիմումին (1)

Հասանելիություն ունենալու իրավունքի 3 հիմնական բաղադրիչները (15-րդ հոդվածի կառուցվածքը)		
Հաստատում, թե արդյոք անձնական տվյալները մշակվում են, թե ոչ.	Անձնական տվյալներին հասանելիություն	Նպատակների, ստացողների վերաբերյալ լրացուցիչ տեղեկություններ և այլն (15(1)«ա»-«ը» հոդված)

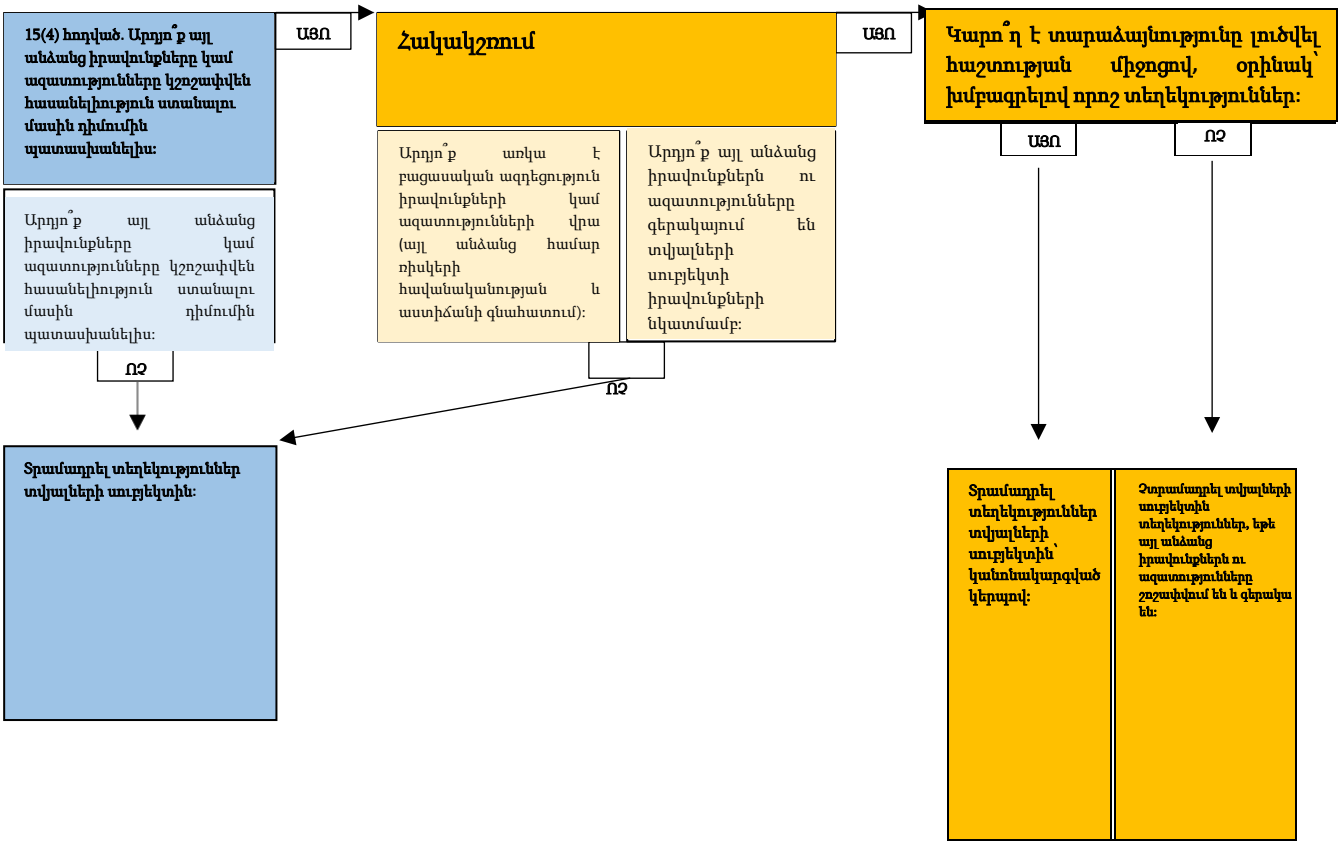
Քայլ 2. Ինչպե՞ս պատասխանել դիմումին (2)

Ձեռնարկել նպատակահարմար միջոցներ			
12(1) հոդված. հակիրճ, թափանցիկ, հասկանալի և հեշտ հասանելի	12(2) հոդված. դյուրացնել հասանելիություն ունենալու իրավունքի իրացումը		
Ընտրել տարբեր միջոցները	Տրամադրել կրկնօրինակը, եթե կողմերն այլ համաձայնության չեն գալիս (15(3) հոդված)	Հարկ եղած դեպքում կիրառել բազմաշերտ մոտեցում (առավել արդիական է առցանց միջավայրում)	Ժամկետ՝ առանց անհարկի ձգձգումների, ցանկացած դեպքում մեկ ամսվա ընթացքում (բացառիկ դեպքերում ժամկետի երկարաձգում ևս երկու ամսով) (12 (3) հոդված)

Քայլ 2. Ի՞նչպես պատասխանել դիմումին (3)

Ինչպե՞ս կարող է հսկողն առբերել տվյալների սուբյեկտի մասին բոլոր տվյալները:			
Սահմանել որոնման չափանիշներ՝ հիմք ընդունելով տվյալների սուբյեկտի կողմից տրամադրված տվյալները, այլ տեղեկություններ, որոնք հսկողը պահում է տվյալների սուբյեկտի մասին և այն գործոնները, որոնց վրա կառուցված են տվյալները (օրինակ՝ հաճախորդի համարը, IP-հասցեները, մասնագիտական կոչումները, ընտանեկան հարաբերությունները և այլն):	Սահմանել ցանկացած տեխնիկական գործառույթ, որը կարող է հասանելի լինել՝ տվյալներն առբերելու համար:	Որոնել բոլոր SS և SS-ի հետ առնչություն չունեցող համապատասխան հաշվառման համակարգերում:	Կազմել, դուրս բերել կամ այլ կերպ հավաքագրել տվյալների սուբյեկտին վերաբերող տվյալներն այնպես, որ այն ամբողջությամբ արտացոլի մշակման գործընթացը, այսինքն, ներառի տվյալների սուբյեկտին վերաբերող բոլոր անձնական տվյալները և հնարավորություն տա տվյալների սուբյեկտին տեղեկանալ, թե արդյոք իրենց տվյալները մշակվում են և մշակվելու դեպքում ստուգել դրա օրինականությունը: Տեղեկությունների առբերումը կարող է կատարվել յուրաքանչյուր առանձին դեպքում, կամ հարկ եղած դեպքում հսկողի կողմից արդեն իսկ ներդրված՝ ներկառուցված անձեռնմխելության սկզբունքի գործիքի կիրառմամբ:

Քայլ 3. Սահմաններն ու սահմանափակումները ստուգելը (1)



Քայլ 3. Սահմաններն ու սահմանափակումները ստուգելը (2)