ԻՆՖՈՐՄԱՑԻԱՅԻ ԱԶԱՏՈՒԹՅԱՆ ԿԵՆՏՐՈՆ

ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ՆԵՐՔԻՆ ՈՒՂԵՑՈՒՅՑ

Տեղական ինքնակառավարման մարմինների համար

Երևան 2021

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

1. Ընդհանուր դրույթներ 2
2. Անձնական տվյալները և դրանց մշակումը 2
3. Անձնական տվյալների մշակման սկզբունքները 3
3.1 Անձնական տվյալների մշակման օրինականությունը 3
3.2 Անձնական տվյալների մշակման համաչափությունը 5
3.3 Հավաստիության սկզբունք և տվյալների ուղղում, փոփոխում, ոչնչացում 6
4. Տվյալների մշակումը համաձայնության հիման վրա 9
5. Անձնական տվյալների պահպանումը 10
6. Անձնական տվյալների փոխանցումը 11
7. Տվյալների արտահոսքի բացահայտում և զեկուցում 13
8. Տվյալների մշակման թափանցիկությունը և մատչելիությունը: Տվյալների սուբյեկտի իրավունքները 13
9. Անձնական տվյալների պաշտպանության համար պատասխանատու անձ 15
10. Տվյալների մշակման ազդեցության գնահատում 16
11. Անչափահասների անձնական տվյալների մշակման առանձնահատկությունները 16
12. ՏԻՄ աշխատակիցների անձնական տվյալների մշակման առանձնահատկությունները 17
13. Տեսահսկում 17

Անձնական տվյալների մշակման ներքին ուղեցույց
Տեղական ինքնակառավարման մարմինների համար

1. Ընդհանուր դրույթներ

Սույն փաստաթղթի հիմնական նպատակն է ապահովել ՏԻՄ-երի կողմից անձնական տվյալների մշակման համապատասխանությունը ազգային և միջազգային չափանիշներին: Ուղեցույցը ներառում է ՏԻՄ աշխատակիցների[1]՝ անձնական տվյալների պաշտպանությանն առնչվող լիազորությունների շրջանակը՝ կապված ՏԻՄ աշխատակիցների և քաղաքացիների անձնական տվյալների մշակման հետ:

ՏԻՄ-երի կողմից մշակվում են երկու խումբ քաղաքացիների անձնական տվյալներ՝ համայնքապետարանների աշխատակիցների անձնական տվյալները աշխատանքային հարաբերությունների շրջանակում եւ քաղաքացիների անձնական տվյալները՝ վերջիններիս ծառայություններ մատուցելու նպատակով: Այս ուղեցույցն ունի խորհրդատվական բնույթ ՀՀ տեղական ինքնակառավարման մարմինների համար:

2. Անձնական տվյալները և դրանց մշակումը

Անձնական տվյալը անձի մասին բոլոր այն տեղեկություններ են, որոնք թույլ են տալիս կամ կարող են թույլ տալ ուղղակի կամ անուղղակի նույնականացնել անձի ինքնությունը (ճանաչել մարդուն): Օրինակ, մարդու անունը, ազգանունը, լուսանկարը, ծննդյան օրը անձնական տվյալներ են:

Անձնական տվյալների պաշտպանության մասին ՀՀ օրենքի (այսուհետ՝ ԱՏՊ օրենք) 3-րդ հոդվածի համաձայն՝ անձնական տվյալի մշակում է ցանկացած գործողություն(ներ), որը կապված է անձնական տվյալներ հավաքելու, ամրագրելու, մուտքագրելու, համակարգելու, պահպանելու, օգտագործելու, վերափոխելու, վերականգնելու, փոխանցելու, ուղղելու, ոչնչացնելու կամ այլ գործողություններ կատարելու հետ: Օրինակ, ՏԻՄ-ին ուղղված քաղաքացու՝ տեղեկություն ստանալու հարցումը ներառում է նրա անունը, ազգանունը, բնակության հասցեն և այլ անձնական տվյալներ: Հարցումը գրանցելու ընթացքում ՏԻՄ-ը պահպանում է (մուտքագրում է) անձի անձնական տվյալները ու հարցմանը պատասխանելուց հետո պահպանում դրանք իր համակարգերում: Այդ գործողությունները համարվում են անձնական տվյալների մշակում, և պետք

[1] «ՏԻՄ աշխատակից» եզրույթի շրջանակում նկատի ունենք տեղական ինքնակառավարման մարմինների ցանկացած աշխատողի՝ անկախ զբաղեցրած պաշտոնից (հաստիքից), պաշտոնի տեսակից, պայմանագրի տեսակից եւ այլ առանձնահատկություններից:

է կատարվեն օրենքով ու օրենքի հիման վրա ընդունված ենթաօրենսդրական նորմատիվ ակտերին համապատասխան։ Սա վերաբերում է տվյալների ինչպես ավտոմատացված, այնպես էլ ոչ ավտոմատացված մշակմանը։

3. Անձնական տվյալների մշակման սկզբունքները

Անձնական տվյալների մշակումը պետք է կատարվի հետեւյալ սկզբունքներին համապատասխան.

3.1 Անձնական տվյալների մշակման օրինականությունը

ՏԻՄ-երի կողմից անձնական տվյալները մշակվում են օրենքով ուղղակիորեն սահմանված դեպքերում եւ կարգով՝ օրենքով իրենց տրված լիազորությունների շրջանակում: Անձնական տվյալների մշակումը համարվում է օրենքի հիման վրա, եթե այդպիսի տվյալներ մշակելու լիազորությունն ուղղակիորեն նախատեսված է օրենքով:

Այն դեպքում, երբ անհրաժեշտ է, որ ՏԻՄ-ն անձնական տվյալը մշակի համաձայնության հիման վրա, անհրաժեշտ է, որ այդ հնարավորությունը (հայեցողությունը) նույնպես նախատեսված լինի օրենքով:

Օրինականության սկզբունքից է բխում, որ ՏԻՄ-ը անձնական տվյալներ է մշակում միայն **որոշակի, բացահայտ և օրինական նպատակի հասնելու համար**։ Անձնական տվյալների մշակման նպատակը պետք է որոշակիացվի և հստակեցվի ՏԻՄ-ի կողմից նախքան տվյալների մշակումը սկսելը[2]։ Այսպիսով, նախքան անձնական տվյալներ հավաքելը ՏԻՄ-ը պետք է վերհանի եւ արձանագրի անձնական տվյալներ մշակելու նպատակ(ներ)ը և մշակման ենթակա տվյալների շրջանակը (ցանկը)։ Ընդ որում՝ սահմանված նպատակը եւ տվյալների շրջանակը պետք է կապված լինեն օրենսդրությամբ սահմանված ՏԻՄ լիազորությունների իրականացման հետ և լինեն անհրաժեշտ նպատակին հասնելու համար։ Օրինակ, եթե ՏԻՄ-ը անձնական տվյալ է հավաքում քաղաքացիներից մանկապարտեզների առցանց հերթագրման նպատակով, ապա տվյալների մշակումը պետք է բացառապես բխի այդ ծառայության մատուցման անհրաժեշտությունից։

Թե՛ քաղաքացիների, թե՛ ՏԻՄ աշխատակիցների անձնական տվյալները մշակվում են օրինական եւ որոշակի նպատակներով եւ առանց անձի համաձայնության չեն կարող օգտագործվել այլ նպատակներով: Անձնական տվյալների մշակման նպատակի սահմանափակումը նշանակում է, որ

[2] Տես՝ 29-րդ հոդվածի ուժով աշխատանքային խմբի (2013) թիվ 03/2013 կարծիքը նպատակի սահմանափակման վերաբերյալ, ԱԽ 203, Բրյուսել, 2013թ. ապրիլի 2։

անձնական տվյալների մշակման օրինականությունը կախված կլինի մշակման նպատակներից[3]։

Նպատակի սահմանափակման սկզբունքից բխում է, որ անձնական տվյալները կարող են մշակվել միայն այն նպատակով, որը սահմանվել էր մինչ տվյալների հավաքագրումը։ Օրինակ, եթե ՏԻՄ վարչական շենքում տեղադրվել է տեսահսկման համակարգ անվտանգության ապահովման նպատակով, ուրեմն դրա միջոցով մշակվող անձնական տվյալները պետք է օգտագործվեն բացառապես այդ նպատակով եւ չեն կարող, օրինակ, օգտագործվել ուշացումների համար ՏԻՄ աշխատակցին կարգապահական տույժի ենթարկելու նպատակով։ Ինչպես նաեւ, անձնական տվյալները չեն կարող նախապես հավաքվել և պահպանվել ապագա հնարավոր նպատակների համար, եթե դա չի պահանջվում օրենսդրությամբ։

ՏԻՄ աշխատակիցը չի կարող ծառայողական կամ աշխատանքային պարտականությունները կատարելու նպատակով իրեն վստահված անձնական տվյալներն օգտագործել ծառայողական կամ աշխատանքային նպատակների հետ չկապված այլ, այդ թվում՝ անձնական նպատակներով։

Անձնական տվյալները պետք է պահպանվեն որոշակի և օրինական նպատակների համար ու չօգտագործվեն այլ նպատակներով[4]։ Այլ նպատակով տվյալների հետագա օգտագործման համար անհրաժեշտ է լրացուցիչ իրավական հիմք, եթե մշակման նոր նպատակը համատեղելի չէ սկզբնական նպատակին։

Նպատակի բացահայտ լինելը նշանակում է, որ տվյալների սուբյեկտի համար պետք է հայտնի լինի, թե ինչ նպատակով է ՏԻՄ-ը մշակում (հավաքում, պահպանում և այլն) իր անձնական տվյալները։

Արգելվում է չսահմանված կամ անսահմանափակ նպատակներով անձնական տվյալների մշակումը։ Նման դեպքերում անձնական տվյալների մշակումը կհամարվի անօրինական եւ կառաջացնի օրենքով նախատեսված պատասխանատվություն։ Պետք է մշակվեն միայն այն անձնական տվյալները, որոնք **համարժեք են, համապատասխան և չեն գերազանցում այն նպատակի սահմանները, որի համար հավաքվում և մշակվում են**[5]։

[3] Թիվ 108 կոնվենցիա, հոդված 5(բ) և 95/46 Դիրեկտիվ, հոդված 6(1)(բ)։
[4] Թիվ 108 կոնվենցիա, հոդված 5(բ)։
[5] Թիվ 108 կոնվենցիա, հոդված 5(գ) և 95/46 Դիրեկտիվ, հոդված 6.1(գ)։

3.2 Անձնական տվյալների մշակման համաչափությունը

Համաչափության սկզբունքից է բխում, որ անձնական տվյալների մշակման օրինական նպատակին հասնելու միջոցները պետք է լինեն **պիտանի, անհրաժեշտ և չափավոր:**

Համաչափության սկզբունքը պահանջում է անձնական տվյալները մշակելիս պահպանել հետեւյալ երկու պայմանները՝

- Պետք է մշակել միայն տվյալների մշակման նպատակի համար անհրաժեշտ անձնական տվյալներ: Տվյալները նվազագույն քանակով մշակելու սկզբունքի համաձայն՝ կարող են մշակվել միայն այն անձնական տվյալները, որոնք մշակման նպատակի տեսանկյունից համարժեք են, տեղին եւ անհրաժեշտ:
- Տվյալները պետք է պահպանվեն ոչ ավելի, քան տվյալների մշակմամբ հետապնդվող նպատակի իրականացման համար անհրաժեշտ ժամկետը (տվյալները սահմանափակ ժամանակով պահպանելու սկզբունքը):

ՏԻՄ-ը պարտավոր է անձնական տվյալները մշակել այն նվազագույն քանակով, որն անհրաժեշտ է նպատակին հասնելու համար: ՏԻՄ-երը պետք է վերհանի նպատակին հասնելու համար անհրաժեշտ անձնական տվյալների նվազագույն ծավալ: Անհաժեշտ է հավաքել կամ պահել միայն այն տվյալները, որոնք անհրաժեշտ են, եւ առանց որոնց անհնար կլինի հասնել սահմանված նպատակին:
Օրինակ, մանկապարտեզի առցանց հերթագրման համար անհրաժեշտ է մշակել միայն երեխայի ծննդյան վկայականի սերիան և համարը, տրման ամսաթիվը և երեխայի ծննդյան ամսաթիվը: Սրանից զատ այլ տվյալի մշակումն այս նպատակով արգելվում է:

ՏԻՄ-ը պարտավոր է ոչնչացնել կամ ուղեփակել անձնական այն տվյալները, որոնք անհրաժեշտ չեն օրինական նպատակին հասնելու համար: Նպատակի համար ոչ պիտանի տվյալների ոչնչացման մասին առավել մանրամասն ներկայացված է սույն Ուղեցույցի 5-րդ բաժնում:

Արգելվում է անձնական տվյալների մշակումը, եթե տվյալները մշակելու նպատակին հնարավոր է հասնել ապանձնավորված կերպով: Անձնական տվյալները մշակելուց առաջ ՏԻՄ աշխատակիցը պետք է որոշի՝արդյոք և որքանով է անհրաժեշտ անձնական տվյալների մշակումը՝ սահմանված նպատակին հասնելու համար: Եթե նպատակը թույլ է տալիս, պետք է օգտագործվեն անանուն կամ վիճակագրական տվյալներ, այսինքն ապանձնավորված տվյալներ:

Անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան

անհրաժեշտ է դրանց նախօրոք որոշված նպատակին հասնելու համար: Օրինակ, եթե քաղաքացին վեբ կայքի միջոցով գրանցվել է այցելության մատյանում, ապա գրանցումը պետք է հեռացվի այցելության ավարտից հետո: Բացառություն են կազմում այն տվյալները, որոնք ամրագրված են փաստաթղթի տեսքով և դրանց պահպանման ժամկետը որոշված է «Արխիվային գործի մասին» ՀՀ օրենքով:

3.3 Հավաստիության սկզբունք և տվյալների ուղղում, փոփոխում, ոչնչացում

Մշակվող անձնական տվյալները պետք է լինեն ամբողջական, ճշգրիտ, պարզ և հնարավորինս թարմացված:

Մշակողը չպետք է օգտագործի այդ տվյալները առանց քայլեր ձեռնարկելու և ողջամտորեն երաշխավորելու, որ այդ տվյալները ճշգրիտ են և թարմացված: Տվյալների ճշգրտությունը երաշխավորելու պարտավորությունը պետք է դիտարկվի տվյալների մշակման նպատակի հետ կապված[6]:

Տվյալների սուբյեկտը իրավունք ունի պահանջել ուղղել իր անձնական տվյալները, եթե մշակվող տվյալներում առկա են տառասխալներ, թվաբանական սխալներ կամ այլ վրիպակներ, ինչպես նաև, երբ տվյալները թարմացված չեն (օրինակ, երբ քաղաքացին փոխել է իր բնակության հասցեն, անձնագիրը կամ հեռախոսահամարը):

ՏԻՄ-ը պարտավոր է տվյալների սուբյեկտի[7] դիմումն ստանալուց հետո 3 աշխատանքային օրվա ընթացքում կատարել պահանջվող գործողությունը, իսկ մերժելու դեպքում՝ դիմումը ստանալու օրվանից հինգ օրվա ընթացքում տրամադրել պատճառաբանված գրավոր որոշում:

Տվյալների սահմանափակ պահպանման սկզբունքի համաձայն՝ տվյալները պետք է պահպանվեն «այնպիսի եղանակով, որը թույլ է տալիս նույնականացնել տվյալների սուբյեկտներին՝ ոչ ավելի երկար ժամանակով, քան անհրաժեշտ է այն նպատակների իրագործման համար, որոնց համար այդ տվյալները հավաքվել կամ մշակվել են»[8]: Այս սկզբունքը նախատեսված է թիվ 108 Արդիականացված կոնվենցիայով[9]: Հետևաբար, տվյալները պետք է ջնջվեն նպատակին հասնելուն պես: Տվյալները կարող են ապանձնավորվել, եթե մշակողը ցանկանում է դրանք պահել սահմանած ժամկետից հետո և երբ տվյալներն այլևս չեն ծառայում իրենց սկզբնական նպատակին[10]:

---

[6] Տվյալների պաշտպանության եվրոպական իրավունքի ձեռնարկ, Հիմնարար իրավունքների ԵՄ գործակալություն, 2014թ. և Եվրոպայի խորհուրդ 2014թ., էջ 71:
[7] Տվյալների սուբյեկտ հասկացությունը վերաբերում է ցանկացած անհատի, անկախ նրա քաղաքացիությունից կամ բնակության վայրից:
[8] Թիվ 108 կոնվենցիա, հոդված 5(ե) և 95/46 Դիրեկտիվ, հոդված 6.1(ե):
[9] Թիվ 108 արդիականացված կոնվենցիա, CAHDATA(2014)RAP03Abr, հոդված 5.4(ե):
[10] Տվյալների պաշտպանության եվրոպական իրավունքի ձեռնարկ, Հիմնարար իրավունքների ԵՄ գործակալություն, 2014թ. և Եվրոպայի խորհուրդ 2014թ., էջ 73:

«Անձնական տվյալների ոչնչացումը» սահմանված է ՀՀ ԱՏՊ օրենքի 3-րդ հոդվածի 1-ին մասի 11-րդ կետում որպես՝ գործողություն, որի արդյունքում հնարավոր չէ վերականգնել տեղեկատվական համակարգում առկա անձնական տվյալների բովանդակությունը: Տվյալները փոփոխելու և ոչնչացնելու ընդհանուր պայմանները ներկայացված են ՀՀ ԱՏՊ օրենքի 20-րդ հոդվածի 2-րդ մասում:[11]

Անձնական տվյալները ոչնչացվում են այն անձի կողմից, ով պատասխանատու է տվյալները մշակելու համար: Անձնական տվյալների ոչնչացման եղանակը (գործողությունը) կապված է տվյալների ամրագրման միջավայրից (կրիչից): Տվյալների ոչնչացման մասին կազմվում է արձանագրություն, որտեղ նշվում է՝ ինչ տեսակի տվյալներ են ոչնչացվել (առանց նշելու բուն տվյալները), ինչ եղանակով, երբ և ում կողմից: Արձանագրությունը հաստատում է ՏԻՄ ղեկավարը:

ՏԻՄ-ում անձնական տվյալների մշակման օրինականությունն ապահովելու համար չափազանց կարևոր է իրականացնել մշակվող (պահպանվող) անձնական տվյալների ժամկետների ու արդիականության մշտադիտարկում: Մշտադիտարկումը պետք է օգնի ՏԻՄ-ի անձնական տվյալների համար պատասխանատու անձանց պարզել՝ արդյոք տվյալների բազաներում պահպանված անձնական տվյալները անհրաժեշտ են և օգտագործվում են այն նպատակների համար, որոնց համար դրանք մշակվել են: Ինչպես նաև, մշտադիտարկումը կարող է օգնել անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնյաներին գնահատել պահպանվող տվյալների արդիականությունը և անհրաժեշտություն դեպքում քայլեր ձեռնարկել այդ տվյալներն արդիականացնելու ուղղությամբ:

Մշտադիտարկման արդյունքները ցանկալի է գրանցել անձնական տվյալների գույքագրման մատյանում: Անձնական տվյալների գույքագրման մատյան վարելն օրենսդրությամբ պարտադիր չէ, սակայն համարվում է լավագույն պրակտիկաներից մեկը: Ակնհայտ է, որ անձնական տվյալների մասին նորմատիվ բազայի ձևավորման ու համապատասխան օրենսդրական պահանջների ընդունման պահին ՏԻՄ-երն արդեն իսկ ունեցել են անձնական տվյալների բազաներ՝ մասամբ էլեկտրոնային, մասամբ թղթային կրիչների վրա: Այն պահին, երբ ՏԻՄ ղեկավարությունը գիտակցում ու քայլել է ձեռնարկում իր տնօրինման ներքո գտնվող անձնական տվյալների մշակման օրինականության ապահովման ուղղությամբ, այն կարող է իրականացնել այդ բազաների հաշվառում:

[11] Որոշ դեպքերում ոչնչացման կոնկրետ տեխնիկական պայմանները սահմանված են ոլորտային իրավական ակտերով, օրինակ, ՀՀ կառավարության 2015 թվականի 1093-Ն որոշման 28-րդ կետը կամ ՀՀ կառավարության 2020 թվականի 298-Ն որոշման 50-54-րդ կետեր:

Անձնական տվյալների գրանցամատյան վարելը չի նշանակում, որ հաշվառվում և պարբերաբար ստուգվում են տվյալների բազաներում առկա բոլոր տվյալները: Սկզբնական հաշվառումը կարող է ներառել բազայի անվանումը, երբ է այն ստեղծվել, ստեղծման իրավական հիմքերը, բազային թարմացման (տվյալների արդիականացման) պարբերականությունը ըստ ստեղծման նպատակների, օրենսդրական ակտի կամ եթե նման պարբերականություն սահմանված չէ, ապա առավել տրամաբանական ժամկետը: Մատյանում ցանկալի է նշել պատասխանատու անձին կամ մասնագետին ըստ հաստիքացուցակի, ինչպես նաև բազայի տեսակն ըստ հասանելության ու գաղտնիության (հանրային կամ խորհրդապահական):

Հետագա տարեկան մշտադիտարկման արդյունքում մատյանում կատարվում եմ գրառումներ այն մասին, թե արդյոք տվյալների բազան դեռ անհրաժեշտ է ու եթե այո, ապա արդիական է այն, թե թարմացման կարիք ունի: Եթե պարզվում է, որ տվյալների բազայի անհրաժեշտությունը վերացել է կամ վերացել են տվյալ բազայի պահպանման օրինական հիմքերը, ապա անձնական տվյալների համար պատասխանատու անձը զեկուցում է դրա մասին ՏԻՄ ղեկավարին: Նախքան անձնական տվյալներ պարունակող բազան ոչնչացնելը ցանկալի է խորհրդակցել անձնական տվյալների պաշտպանության համար պատասխանատու պետական մարմնի՝ ՀՀ ԱՆ Անձնական տվյալների պաշտպանության գործակալության հետ:

Համոզվելով, որ անձնական տվյալների բազան ենթակա է ոչնչացման, ՏԻՄ ղեկավարը կազմում է իր նախագահությամբ անձնական տվյալների ոչնչացման հանձնաժողով, ընդունում է տվյալները ոչնչացնելու վերաբերյալ հրաման: Հանձնաժողովի անդամների մասնակցությամբ կազմվում է տվյալների ոչնչացման ակտ: Հանձնաժողովի անդամները պետք է համոզվեն, որ տվյալների բազան այլևս գոյություն չունի ու հաստատեն դա՝ ստորագրելով ակտը:

Եթե անձնական տվյալների բազա մուտքի իրավունք ունեն նաև այլ պետական կամ տեղական ինքնակառավարման մարմիններ, ցանկալի է նրանց նույնպես տեղեկացնել, որ կազմակերպությունը պլանավորում է ոչնչացնել անձնական տվյալների բազան: Հիմնավոր առարկությունների դեպքում ցանկալի է հարցը քննարկել ԱՏՊ գործակալության հետ և հաշվի առնել վերջինիս կարծիքը վերջնական որոշում ընդունելիս:

4. Տվյալների մշակումը համաձայնության հիման վրա

Անձնական տվյալների մշակումը կարող է իրականացվել տվյալների սուբյեկտի ազատ, որոշակի, տեղեկացված և հստակ համաձայնության հիման վրա: Համաձայնությունը սահմանում է որպես՝ «տվյալների սուբյեկտի կողմից որոշակի և տեղեկացված հիմունքներով արված ազատ կամահայտնություն, որով նա տալիս է իր հավանությունը՝ իրեն վերաբերող անձնական տվյալները մշակելու համար[12]:

Համաձայնությունը վավերական համարվելու համար անհարժեշտ է երեք բաղադրիչ, որոնց նպատակն է երաշխավորել, որ տվյալների սուբյեկտն իսկապես տվել է իր համաձայնությունը իր տվյալների օգտագործման համար.

- տվյալների սուբյեկտը համաձայնություն տալիս չպետք է ճնշման ենթարկված լինի (այսինքն՝ համաձայնությունը ազատ տրված է),
- տվյալների սուբյեկտը պետք է պատշաճ տեղեկացված լինի համաձայնության առարկայի և հետևանքների մասին (այսինքն՝ տեղեկացված),
- համաձայնության շրջանակը պետք է կոնկրետ լինի (այսինքն՝ տվյալների սուբյեկտի համաձայնությունը պետք է տրված լինի կոնկրետ նպատակով սպառիչ թվարկված անձնական տվյալների մշակման վերաբերյալ)[13],
- տվյալների սուբյեկտը համաձայնությունը պետք է տա հստակ ձևով (այսինքն՝ տվյալների սուբյեկտի կողմից համաձայնություն տալու փաստը չպետք է առաջացնի կասկած կամ երկիմաստություն):

Անձնական տվյալների պաշտպանության ոլորտում համաձայնությունը վավերական կլինի, միայն եթե այս բոլոր չորս պահանջները բավարարվեն միաժամանակ:

Համաձայնություն տալուց առաջ տվյալների սուբյեկտը պետք է տեղեկացվի, ինչպես նշվում է սույն Ուղեցույցի 7-րդ բաժնում: Համաձայնությունը պետք է ստացվի գրավոր կամ էլեկտրոնային եղանակով՝ փաստաթղթավորման նպատակներով: Որոշ հանգամանքներում, ինչպիսիք են հեռախոսային խոսակցությունները, համաձայնությունը կարող է տրվել բանավոր: Անհրաժեշտ է ապահովել, որ տրված համաձայնությունը պատշաճ կերպով փաստաթղթավորվի:

«Տվյալների սուբյեկտի համաձայնությունը տրվում է գրավոր կամ էլեկտրոնային եղանակով՝ հաստատված էլեկտրոնային թվային ստորագրությամբ, բանավոր համաձայնության դեպքում՝ այնպիսի հավաստի գործողությունների միջոցով,

[12] 95/46 Դիրեկտիվ, հոդված 2(ը):

[13] Տվյալների պաշտպանության եվրոպական իրավունքի ձեռնարկ, Հիմնարար իրավունքների ԵՄ գործակալություն, 2014թ. և Եվրոպայի խորհուրդ 2014թ., էջ 56:

որոնք ակնհայտորեն կվկայեն տվյալների սուբյեկտի՝ անձնական տվյալները օգտագործելու համաձայնության մասին»:

Համաձայնությունը կարող է տրվել գրավոր՝ հաստատված ստորագրությամբ, բանավոր, գործողության միջոցով, որն ակնհայտ վկայում է համաձայնության մասին: Թեեւ համաձայնությունը կարող է տրվել ցանկացած ձեւով, սակայն այն պետք է հստակ արտացոլի տվյալների սուբյեկտի կամքը իր անձնական տվյալների մշակման վերաբերյալ: Այսինքն, համաձայնությունը պետք է լինի «միանշանակ»: Սա նշանակում է, որ չպետք է որեւէ կասկած մնա, որ տվյալների սուբյեկտի համաձայնությունն ուղղված է հենց անձնական տվյալների մշակմանը: Այլ կերպ ասած՝ տվյալների սուբյեկտի կամահայտնությունը, որով նա տալիս է իր հավանությունն անձնական տվյալների մշակման վերաբերյալ, պետք է միանշանակորեն վկայի տվյալների սուբյեկտի մտադրության վերաբերյալ, իսկ եթե կա տվյալների սուբյեկտի մտադրության վերաբերյալ ողջամիտ կասկած, ապա համաձայնությունը չի կարող համարվել միանշանակորեն տրված:

Համաձայնության՝ «տեղեկացված» լինելու չափանիշից բխում է, որ անձնական տվյալների սուբյեկտի համաձայնությունը պետք է հիմնված լինի անձնական տվյալների մշակման հանգամանքները եւ հետեւանքները գիտակցելու եւ հասկանալու, անձնական տվյալների մշակման (մշակվող տվյալների, մշակման նպատակի, այլն անձանց հնարավոր փոխանցման, տվյալների սուբյեկտի իրավունքների եւ այլնի) վերաբերյալ ճշգրիտ եւ լիարժեք տեղեկությունների վրա: Ընդ որում, տեղեկությունները պետք է հասանելի, հասկանալի եւ տեսանելի լինեն տվյալների սուբյեկտի համար, այլ ոչ թե «հասանելի ինչ-որ տեղ»:

Տվյալների սուբյեկտի համաձայնությունը ստանալու փաստն ապացուցելու (...) պարտականությունը կրում է մշակողը: Համաձայնության ձեռք բերման ապացուցման բեռն ընկնում է ՏԻՄ-ի վրա:

Տես՝ համաձայնության օրինակելի ձեւը Հավելված 1-ում, որում մասնավորապես նշվում են մշակվող տվյալների շրջանակը, մշակման նպատակը, այն գործողությունները, որոնք պետք է կատարվեն այդ տվյալների հետ, այն անձանց շրջանակը, ում հասու են դառնալու տվյալները, այն ժամկետը, որի սահմաններում պահպանելու են տվյալները:

5. Անձնական տվյալների պահպանումը

Անձնական տվյալները պետք է պահպանվեն այնպես, որ բացառվի տվյալների սուբյեկտի հետ դրանց նույնականացումն ավելի երկար ժամկետով, քան

անհրաժեշտ է դրանց նախօրոք որոշված նպատակներին հասնելու համար: ՏԻՄ-երը պարբերաբար պետք է իրականացնեն ոչ պիտանի անձնական տվյալները սահմանված ժամկետի ավարտից հետո բացահայտելու, վերացնելու կամ ջնջելու գործընթաց: Օրինակ, ՏԻՄ աշխատակցի հետ աշխատանքային պայմանագիրը լուծելուց հետո գործատուն պարտավոր է ոչնչացնել կամ ապանձնավորել աշխատողի բոլոր այն անձնական տվյալները, որոնց մշակման նպատակները սպառվել են, բացառությամբ այն տվյալների որոնց պահպանման ժամկետները նախատեսված են օրենքով:

Հատուկ կատեգորիայի[14] եւ կենսաչափական անձնական տվյալներ[15] մշակելու պարագայում որոշակի առանձնահատկություններ են սահմանվում, և դրանց տրվում է առանձնացված կարգավիճակ: Միաժամանակ, այս կատեգորիայի անձնական տվյալների համար ապահովվում է պահպանության առավել բարձր մակարդակ՝ կիրառելով պահպանության լրացուցիչ երաշխիքներ: Մասնավորապես, էլեկտրոնային տեսքով պահպանվող կենսաչափական անձնական տվյալների դեպքում պետք է օգտագործվեն գաղտնագրման ծրագրեր: Գաղտնագրման ծրագրերի տեսակները և գաղտնագրման բանալիների երկարությունը պետք է որոշի ՏՏ մասնագետը՝ հաշվի առնելով միջազգային ստանդարտները, օրինակ՝ FIPS-140 համապատասխանող ստանդարտները և ալգորիթմները:

Տվյալների պահպանումն ԱՏՊ օրենքի իմաստով տվյալների մշակում է, ուստի պահպանմանը վերաբերում են օրենքի այն բոլոր ընդհանուր կանոնները, որոնք վերաբերում են տվյալների մշակմանը: Ամեն դեպքում, կենսաչափական անձնական տվյալների մասով կիրառելի են ԱՏՊ օրենքից բխող՝ կենսաչափական անձնական տվյալների նյութական կրիչներին և տեղեկատվական համակարգերից դուրս այդ անձնական տվյալները պահպանելու տեխնոլոգիաներին ներկայացվող պահանջները, որոնք սահմանվել են Կառավարության 2015 թվականի 1175-Ն որոշմամբ:

6. Անձնական տվյալների փոխանցումը

Անձնական տվյալների փոխանցումը երրորդ անձանց սահմանվում է որպես «անձնական տվյալները որոշակի կամ անորոշ շրջանակի այլ անձանց փոխանցելուն կամ դրանց հետ ծանոթացնելուն ուղղված գործողություն, այդ թվում՝ զանգվածային լրատվության միջոցներով անձնական տվյալները

[14] Հատուկ կատեգորիայի անձնական տվյալներ՝ անձի ռասայական, ազգային պատկանելությանը կամ էթնիկ ծագմանը, քաղաքական հայացքներին, կրոնական կամ փիլիսոփայական համոզմունքներին, արհեստակցական միությանն անդամակցությանը, առողջական վիճակին ու սեռական կյանքին վերաբերող տեղեկություններ:

[15] Կենսաչափական տվյալ - կենսաչափական անձնական տվյալներ՝ անձի ֆիզիկական, ֆիզիոլոգիական եւ կենսաբանական առանձնահատկությունները բնութագրող տեղեկություններ:

հրապարակելը, տեղեկատվական հաղորդակցման ցանցերում տեղադրելը կամ այլ եղանակով անձնական տվյալներն այլ անձի մատչելի դարձնելը։

Առանց անձնական տվյալների սուբյեկտի համաձայնության մշակողը կարող է անձնական տվյալները փոխանցել երրորդ անձանց կամ տվյալներից օգտվելու հնարավորություն տրամադրել, եթե դա ուղղակիորեն նախատեսված է օրենքով։
Առանց տվյալների սուբյեկտի համաձայնության անձնական տվյալների փոխանցման պայմաններն են՝

- Փոխանցումը նախատեսված է օրենքով և
- Երրորդ կողմն ունի պաշտպանության բավարար մակարդակ։

ՀՀ ԱՏՊ օրենքում «երրորդ անձ (կողմ)» հասկացությունը սահմանված է որպես «ցանկացած անձ, մարմին, հիմնարկ կամ կազմակերպություն, որը չի հանդիսանում տվյալների սուբյեկտ, անձնական տվյալների մշակող կամ լիազորված անձ, և որի իրավունքները կամ օրինական շահերը շոշափվում կամ կարող են շոշափվել անձնական տվյալները մշակելու արդյունքում»։

Նախատեսվում է երրորդ կողմին անձնական տվյալների փոխանցման երկու դեպք։ Առաջին դեպքն այն է, երբ «տվյալներ մշակողը հանդիսանում է օրենքով կամ միջպետական պայմանագրով սահմանված հատուկ կատեգորիայի անձնական տվյալներ մշակող, այդ տեղեկության փոխանցումը ուղղակիորեն նախատեսված է օրենքով և ունի բավարար պաշտպանության մակարդակ»։

Երկրորդ դեպքը կարող է վերաբերել տվյալների սուբյեկտի կենսական շահերին, երբ «օրենքով նախատեսված բացառիկ դեպքերում հատուկ կատեգորիայի անձնական տվյալները կարող են փոխանցվել տվյալների սուբյեկտի կյանքի, առողջության կամ ազատության պաշտպանության համար։

Տվյալների սուբյեկտի կենսական շահերն ակնհայտորեն հաշվի են առնված որպես տվյալների մշակումը հիմնավորող վավերական պատճառ[16]։

ՏԻՄ-ի տնօրինության տակ գտնվող անձնական տվյալներն այլ պետական մարմիններին կարող են փոխանցվել միայն օրենքներով ուղղակիորեն նախատեսված դեպքերում։

Պետական մարմինների տվյալների բազաներում մշակվող անձնական տվյալներն էլեկտրոնային եղանակով փոխանցման կարգը սահմանվում է ՀՀ կառավարության որոշմամբ (19 դեկտեմբերի 2019 թվականի N 1849-Ն):

Եթե ՏԻՄ աշխատողին անհրաժեշտ է խորհրդակցել այլ անձանց (այդ թվում՝ այլ աշխատողի կամ այլ մարմնի աշխատողի) հետ, եւ այդ նպատակով պետք է փոխանցի ծառայողական կամ աշխատանքային նպատակներով իրեն

[16] Տվյալների պաշտպանության եվրոպական իրավունքի ձեռնարկ, Հիմնարար իրավունքների ԵՄ գործակալություն, 2014թ. և Եվրոպայի խորհուրդ 2014թ., էջ 83։

վստահված կամ հայտնի դարձած եւ ոչ հանրամատչելի անձնական տվյաներ պարունակող փաստաթղթեր, ապա ՏԻՄ աշխատակիցը տվյալներն այլ գերատեսչություն պետք է փոխանցի ապանձնավորված կերպով եւ նվազագույն քանակով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար:

7. Տվյալների արտահոսքի բացահայտում և զեկուցում

Էլեկտրոնային համակարգերից անձնական տվյալների արտահոսք լինելու դեպքում ՏԻՄ-ը պետք է անհապաղ ՀՀ ԱՆ ԱՏՊ գործակալությանը տեղեկացնի: ՏԻՄ-ը պարտավոր է այդ մասին անհապաղ հրապարակել հայտարարություն՝ միաժամանակ արտահոսքի վերաբերյալ հայտնելով Հայաստանի Հանրապետության ոստիկանությանը և ՀՀ ԱՆ անձնական տվյալների պաշտպանության գործակալությանը:

Նմանապես, ՏԻՄ-ը պարտավոր է անհապաղ տեղեկացնել հետեւյալ դեպքերում.

- անձնական տվյալների ոչ պատշաճ փոխանցում երրորդ անձանց,
- երրորդ անձանց կողմից անձնական տվյալների չթույլատրված մուտք,
- անձնական տվյալների կորուստ, արտահոսք:

Անձնական տվյալների հետ իրականացվող անօրինական գործողություններ հայտնաբերելու դեպքում ՏԻՄ-ը պարտավոր է անհապաղ, բայց ոչ ուշ, քան երեք աշխատանքային օրվա ընթացքում վերացնել թույլ տված խախտումները: Խախտումները վերացնելու անհնարինության դեպքում մշակողը պարտավոր է անհապաղ ոչնչացնել անձնական տվյալները: Խախտումները վերացնելու կամ անձնական տվյալները ոչնչացնելու մասին մշակողը պարտավոր է երեք աշխատանքային օրվա ընթացքում տեղեկացնել տվյալների սուբյեկտին կամ նրա ներկայացուցչին, իսկ այն դեպքում, երբ հարցումն ստացվել է անձնական տվյալների պաշտպանության լիազոր մարմնից՝ նաև այդ մարմնին:

8. Տվյալների մշակման թափանցիկությունը և մատչելիությունը: Տվյալների սուբյեկտի իրավունքները

Անձնական տվյալների մշակումը պետք է լինի թափանցիկ գործընթաց: Այս պահանջի նպատակն է խուսափել գաղտնի կամ ծածուկ մշակումից (մասնավորապես՝ տվյալների հավաքագրման փուլում): Հակառակ դեպքում տվյալների սուբյեկտը չի կարող վերահսկողություն իրականացնել իր անձնական տվյալների օգտագործման նկատմամբ:
ՏԻՄ-երը տվյալների սուբյեկտներին պետք է տեղեկացնեն, որ իրենց տվյալները մշակվում են օրինական և թափանցիկ ձևով: Մշակումը չպետք է իրականացվի

գաղտնի: Մշակողը պետք է երաշխավորի, որ տվյալների սուբյկետն տեղյակ լինի իր տվյալների մշակման և օգտագործման մասին: Բացի այդ, մշակողը հնարավորինս պետք է գործի այնպես, որպեսզի օպերատիվ կերպով բավարարվեն տվյալների սուբյեկտի ցանկությունները, օրինակ՝ տվյալները փոփոխելու, թարմացնելու վերաբերյալ:

ԱՏՊ ոլորտում տվյալների սուբյեկտն ունի հետեւյալ իրավունքները.

1. **Տեղյակ լինելու իրավունք.** Թափանցիկության սկզբունքից է բխում, որ անձն ունի իր անձնական տվյալների մշակման վերաբերյալ տեղյակ լինելու իրավունք:
2. **Տեղեկություն ստանալու իրավունք.** Այս իրավունքից է բխում, որ տվյալների սուբյեկտն իրավունք ունի ստանալ հստակ, մատչելի, ճշգրիտ տեղեկատվություն այն մասին, թե ինչպես են իր տվյալները մշակվում, ինչ նպատակով ու ծավալով:
3. **Մոռացված լինելու իրավունք.** Սա ներառում է տվյալների սուբյեկտի՝ իր անձնական տվյալները ջնջելու իրավունքը:
4. **Ուղղելու, փոփոխելու իրավունք.** Անձն իրավունք ունի պահանջել ուղղել, փոփոխել իր անձնական տվյալները, եթե դրանք ոչ ճշրգիտ կամ ոչ ամբողջական են:
5. **Առարկելու իրավունք.** Տվյալների սուբյեկտն ունի իր տվյալների մշակմանն առարկելու իրավունք:

Անձն իրավունք ունի անձնական տվյալներ մշակողից ստանալ հետեւյալ տեղեկությունները.

- Նա իրավունք ունի ստանալ մշակվող անձնական տվյալների պատճենները (ինչպես ֆիզիկական, այնպես էլեկտրոնային եղանակով),
-Իրավունք ունի ստանալ տեղեկություններ իր անձնական տվյալները մշակելու հիմքերի և նպատակների մասին,
- Իրավունք ունի տեղեկություն ստանալ տվյալները մշակողի, նրա գտնվելու վայրի մասին, ինչպես նաև այն անձանց շրջանակի մասին, որոնց կարող են փոխանցվել իր անձնական տվյալները,
-Իրավունք ունի իմանալ իր անձնական տվյալները մշակելու ժամկետների վերաբերյալ,
- իրավունք ունի իմանալ նաեւ անձնական տվյալները մշակելու հետևանքով իր համար առաջացող հնարավոր իրավական հետևանքների վերաբերյալ:

Անձնական տվյալների մշակման մասին անձին հարցման հիման վրա տվյալները պետք է տրամադրվեն 5-օրյա ժամկետում: Անձնական տվյալի սուբյկետին տեղեկությունները տրամադրվում են անվճար: Անձին տեղեկությունները չպետք է վաճառվեն, իսկ որոշակի գումար վճարելը պետք է նպատակ ունենա

փոխհատուցելու մշակողի՝ տեղեկությունները տրամադրելու հետ կապված ծախսերը:

Անձը նաև իրավունք ունի պահանջել ջնջել ցանկացած անձնական տվյալ, որն անհրաժեշտ չէ նպատակին հասնելու համար: Միաժամանակ, անձն ունի իր մասին սխալ, ոչ ճշգրիտ տեղեկության ճշգրտման իրավունք: Տվյալների սուբյկետը իրավունք ունի ՏԻՄ-ից պահանջել ուղղել իր անձնական տվյալները, եթե մշակվող տվյալներում առկա են տառասխալներ, թվաբանական սխալներ կամ այլ վրիպակներ, ինչպես նաև, երբ տվյալները թարմացված չեն:

ՏԻՄ-ը պարտավոր է քաղաքացու դիմումն ստանալուց հետո 3 աշխատանքային օրվա ընթացքում կատարել պահանջվող գործողությունը, իսկ մերժելու դեպքում՝ դիմումը ստանալու օրվանից հինգ օրվա ընթացքում տրամադրել պատճառաբանված գրավոր որոշում:

Տվյալների սուբյեկտը պետք է տեղեկացվի, թե ինչպես են մշակվում իր տվյալները: Ընդհանուր առմամբ, անձնական տվյալները պետք է հավաքվեն ուղղակիորեն տվյալ անձից: Տվյալները հավաքելիս տվյալների սուբյեկտը պետք է կա՛մ տեղյակ լինի մշակման մասին, կա՛մ տեղեկացված լինի հետևյալի մասին.

- Տվյալների մշակման նպատակը և օրինական հիմքը, մշակվող տվյալների ցանկը.
- Անձնական տվյալների հավանական օգտագործողների շրջանակը.
- Երրորդ կողմեր, որոնց կարող են փոխանցվել տվյալները.

Հարցման օրինակելի ձևը տես Հավելված 2-ում:

9. Անձնական տվյալների պաշտպանության համար պատասխանատու անձ

Յուրաքանչյուր ՏԻՄ մարմնում պետք է նշանակվի Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձ: Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձը՝

- ապահովում է «Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքով սահմանված՝ անձնական տվյալներ մշակողի պարտականությունների կատարումը,
- ապահովում է պետական մարմնի կապն անձնական տվյալների պաշտպանության լիազոր մարմնի հետ, այդ թվում՝ կազմակերպում անձնական տվյալների մշակման վերաբերյալ խորհրդատվության ստացումը,
- կազմում եւ անձնական տվյալների պաշտպանության լիազոր մարմնի ղեկավարին է ներկայացնում անձնական տվյալների պաշտպանության վերապատրաստման՝ ՏԻՄ ներկայացուցիչների ցուցակը,

- ապահովում է անձնական տվյալների պաշտպանության վերաբերյալ քաղաքացիների հարցումների եւ այլ գրությունների պատասխանները, անհրաժեշտության դեպքում դրանք ներկայացնում անձնական տվյալների պաշտպանության լիազոր մարմնի կարծիքին,
- իրականացնում է պետական մարմնի կողմից անձնական տվյալների մշակմանը վերաբերող այլ անհրաժեշտ միջոցառումներ:
- Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձի հետ կապ հաստատելու տվյալները (էլեկտրոնային փոստի հասցեն, հեռախոսահամարը) տեղադրվում են տվյալ պետական մարմնի պաշտոնական կայքում:

Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձ չնշանակելու դեպքում անձնական տվյալների պաշտպանության համար պատասխանատու է ՏԻՄ ղեկավարը կամ գլխավոր քարտուղարը՝ կախված տվյալների մշակման դեպքից:

10. Տվյալների մշակման ազդեցության գնահատում

Տվյալների մշակման ազդեցության գնահատման նպատակը տվյալների գաղտնիությանը սպառնացող ռիսկերը բացահայտելն է, գնահատելը, կառավարելը կամ խուսափելը: Գնահատման նպատակը տվյալների պաշտպանության խնդիրները մշակման և ծրագրավորման փուլում հայտնաբերելն է, հետևաբար և դրանք արագ և արդյունավետ կերպով շտկելու կարողությունը: ՏԻՄ-ը իրականացնում է տվյալների սուբյեկտների իրավունքների և հիմնարար ազատությունների վրա նախատեսվող մշակման ազդեցության համապարփակ պարբերաբար վերանայում և գնահատում (առնչվող անձնական տվյալների կատեգորիաների, մշակման շրջանակների, տվյալների ներքին և արտաքին հոսքի, անվտանգության միջոցների համարժեքության և այլնի հետ կապված):

11. Անչափահասների անձնական տվյալների մշակման առանձնահատկությունները

Անչափահասների անձնական տվյալնեի մշակման առանձնահատկությունները սահմանվում են ՀՀ ԱՆ ԱՏՊ գործակալության ընդունած ուղեցույցում՝ https://www.unicef.org/armenia/media/2761/file:

12. ՏԻՄ աշխատակիցների անձնական տվյալների մշակման առանձնահատկությունները

ՏԻՄ աշխատակիցների անձնական տվյալների մշակման առանձնահատկությունները աշխատանքային հարաբերությունների շրջանակում սահմանված են ՀՀ ԱՆ ԱՏՊ գործակալության ընդունած ուղեցույցում: https://www.moj.am/storage/uploads/002employee_guide-10.04.2017.pdf?fbclid=IwAR0nYqvimrSvbg47WwJez3Rpz9bD9xxPtRVmK7tsqfdX07sEiNk6UEMn5S8:

13. Տեսահսկում

ՏԻՄ վարչական շենքում տեսահսկում իրականացնելու կանոններն ու ընթացակարգերը սահմանվում են ԱՏՊ գործակալության մշակած եւ ընդունած տեսահսկման ընդհանուր ուղեցույցում՝ https://www.moj.am/storage/uploads/001Video_surveillance_guide.pdf?fbclid=IwAR0OmrghQqWfGuBP4YGtsVhz8cangIdMcrxOmTfZ0X9EDfRtVjlIxyN1_SQ