

ՈՒՂԵՑՈՒՅՑ

ՀՀ կրթության, գիտության, մշակույթի և սպորտի նախարարության կողմից անձնական տվյալների մշակման

Սույն ուղեցույցը նպատակ ունի «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի դրույթների հիման վրա սահմանել ՀՀ կրթության, գիտության, մշակույթի և սպորտի նախարարության (այսուհետ՝ նախարարությունը) կողմից անձնական տվյալների մշակման ցուցումներ, այդ թվում՝ անձնական տվյալներ մշակելու անվտանգության ապահովման միջոցների և մշակողի պարտականությունների, այլ պետական մարմիններին անձնական տվյալների փոխանցման, անձնական տվյալների պաշտպանության համար պատասխանատուի, անձնական տվյալների պաշտպանության իրավունքի վերաբերյալ վերապատրաստման մասին:

1. Անձնական տվյալներ մշակելու հիմքը, տվյալների մշակում նախատեսելը, տվյալներ ստանալը

1) Նախարարության կողմից անձնական տվյալների մշակումը կարող է իրականացվել՝ անձնական տվյալները կարող են հավաքվել, ամրագրվել, մուտքագրվել, համակարգվել, կազմակերպվել, պահպանվել, օգտագործվել, վերափոխվել, վերականգնվել, փոխանցվել, ուղղվել, ուղեփակվել, ոչնչացվել, կամ դրանց հետ այլ գործողություն կարող է կատարվել բացառապես օրենքներով (օրենքի մակարդակում) ուղղակիորեն սահմանված դեպքերում և կարգով:

2) Այն պարագայում, երբ անհրաժեշտ է, որ նախարարությունն օգտվի անձնական տվյալի մշակման համաձայնության հիմքերից, անհրաժեշտ է, որ այդ հնարավորությունը (հայեցողությունը) նույնպես նախատեսված լինի օրենքով:

3) Անձնական տվյալների մշակում նախատեսող օրենքներ նախագծելիս, օրենսդրական նախաձեռնություն իրականացնելիս Նախարարությունը պետք է առաջնորդվի անձնական տվյալների մշակման համաչափության սկզբունքով, այդ թվում.

ա. սահմանի անձնական տվյալների մշակման որոշակի նպատակ,

բ. նախատեսի սահմանված նպատակին հասնելու համար անձնական տվյալների մշակման պիտանի, անհրաժեշտ և չափավոր միջոցներ,

գ. նախատեսի սահմանված նպատակին հասնելու համար անհրաժեշտ նվազագույն քանակի անձնական տվյալների մշակում,

դ. չնախատեսի այնպիսի անձնական տվյալների մշակում, որոնք անհրաժեշտ չեն սահմանված նպատակին հասնելու համար,

ե. չնախատեսի անձնական տվյալների մշակում, եթե սահմանված նպատակին հնարավոր է հասնել ապանձնավորված ձևով,

զ. նախատեսի անձնական տվյալների մշակման այնպիսի ժամկետ, որն անհրաժեշտ է սահմանված (այդ թվում՝ արխիվային պահպանության) նպատակին հասնելու համար,

է. նախատեսի կենսաչափական անձնական տվյալների մշակում, եթե սահմանված նպատակը հնարավոր է իրականացնել միայն այդ կենսաչափական տվյալները մշակելու միջոցով:

4) Նախարարությունը կարող է ստանալ կամ ձևավորել անձնական տվյալներ միայն օրենքներով ուղղակիորեն սահմանված դեպքում և կարգով:

2. Անձնական տվյալների անվտանգությունը, տվյալների օգտագործումը

1) Անձնական տվյալների մշակում իրականացնելիս, Նախարարությունն առաջնորդվում է «Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքի 5-րդ գլխի դրույթներով:

2) Նախարարությունը և նախարարության աշխատողները ծառայողական կամ աշխատանքային պարտականությունները կատարելու ընթացքում, ինչպես նաև դրա ավարտից հետո իրենց վստահված անձնական տվյալները կամ անձնական տվյալներ պարունակող փաստաթղթերը ծառայողական կամ աշխատանքային նպատակներով օգտագործելիս պետք է ձեռնարկեն անհրաժեշտ տեխնիկական և կազմակերպչական միջոցառումներ՝ անձնական տվյալների պաշտպանությունն անօրինական օգտագործումից, ձայնագրումից, ոչնչացումից, վերափոխումից, ուղեփակումից, կրկնօրինակումից, տարածումից և այլ միջամտությունից պաշտպանելու համար: Սա վերաբերում է ինչպես նախարարության աշխատողների աշխատանքի կազմակերպմանը, այնպես էլ նրանց կողմից օգտագործվող համակարգչային և այլ տեխնիկական միջոցների պաշտպանվածությանը:

3) Տեղեկատվական համակարգերում անձնական տվյալները մշակելու անվտանգությունն ապահովելուն ներկայացվող պահանջները սահմանվում են ՀՀ կառավարության որոշմամբ:

4) Նախարարության աշխատողը չի կարող ծառայողական կամ աշխատանքային պարտականությունները կատարելու նպատակով իրեն վստահված անձնական տվյալներն օգտագործել ծառայողական կամ աշխատանքային նպատակների հետ չկապված այլ, այդ թվում՝ անձնական նպատակներով:

5) Եթե նախարարության աշխատողին ծառայողական կամ աշխատանքային նպատակներով անձնական տվյալներ կամ անձնական տվյալներ պարունակող փաստաթղթեր օգտագործելիս անհրաժեշտ է օգտվել անձնական (ոչ ծառայողական) տեխնիկական միջոցներից (այդ թվում՝ հեռախոս, համակարգիչ և այլն), ապա նախարարության աշխատողն անձնական տեխնիկական միջոցների համար պետք է ապահովի այն նույն պաշտպանվածությունը, ինչ ապահովված է ծառայողական տեխնիկական միջոցների համար: Հակառակ պարագայում անձնական տեխնիկական միջոցներով ծառայողական կամ աշխատանքային պարտականությունների համար անհրաժեշտ անձնական տվյալների մշակումն արգելվում է:

6) Եթե նախարարության 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 վստահված կամ հայտնի դարձած և ոչ հանրամատչելի անձնական տվյալներ պարունակող փաստաթղթեր, ապա նախարարության աշխատողը պետք է առաջնորդվի «Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքի 5-րդ գլխի դրույթներով, մասնավորապես՝ տվյալներն այլ գերատեսչություն փոխանցել ապանձնավորված կերպով և նվազագույն քանակով, որն անհրաժեշտ է օրինական նպատակներին հասնելու համար:

7) Նախարարության աշխատողը էլեկտրոնային փաստաթղթաշրջանառության համակարգից (օրինակ՝ «Mulberry» համակարգ) օգտվելիս պետք է սահմանափակի այլ աշխատողների հասանելիությունը ծառայողական կամ աշխատանքային նպատակներով իրեն վստահված կամ հայտնի դարձած և ոչ հանրամատչելի անձնական տվյալներ պարունակող փաստաթղթերին՝ համակարգի կարգավորումների միջոցով անձնական տվյալներ պարունակող փաստաթղթերը հասանելի դարձնելով միայն այն ծավալով և այն աշխատակիցներին, որոնք իրենց աշխատանքային պարտականություններից ելնելով կարող են կամ պետք է առնչվեն տվյալ փաստաթղթին:

8) Նախարարության աշխատողը, ծառայողական կամ աշխատանքային նպատակներով իրեն վստահված կամ հայտնի դարձած և ոչ հանրամատչելի անձնական տվյալների արտահոսքը կանխելու նպատակով, չպետք է կողմնակի անձանց (այդ թվում՝ պետական համակարգի այլ աշխատողներին) փոխանցի էլեկտրոնային փաստաթղթաշրջանառության համակարգի (օրինակ՝ «Mulberry» համակարգի) իր անձնական էջ մուտք գործելու տվյալները՝ մուտքանունը և գաղտնաբառը:

9) Նախարարության աշխատողի՝ աշխատանքից ազատվելու պարագայում անհրաժեշտ է արգելափակել տվյալ անձի էլեկտրոնային փաստաթղթաշրջանառության համակարգի անձնական էջը՝ նրա կողմից այլ տեխնիկական սարքավորումներից և անձնական նպատակներով համակարգ մուտք գործելը կանխելու համար:

10) Վերոնշյալ կանոնները վերաբերում են նաև նյութական կրիչով (ներառյալ՝ թղթային տարբերակով) կամ էլեկտրոնային փոստի միջոցով ծառայողական կամ աշխատանքային նպատակներով նախարարության աշխատողին վստահված կամ հայտնի դարձած և ոչ հանրամատչելի անձնական տվյալների հասանելիության սահմանափակմանը՝ նյութական կրիչի կամ էլեկտրոնային փոստի մատչելիությանը վերաբերելի միջոցներով: Մասնավորապես, նախարարության աշխատողը պետք է օգտվի ծառայողական էլեկտրոնային փոստից (եթե այդպիսին առկա է) կամ այնպիսի էլեկտրոնային փոստից, որն ապահովում է տվյալների բավարար պաշտպանության մակարդակ, էլեկտրոնային փոստի մուտքանունը և գաղտնաբառը չտրամադրի այլ անձանց, անձնական տվյալներ պարունակող նյութական կրիչը աշխատասենյակում (աշխատասենյակին) պահի այնպես, որ կանխվի անձնական տվյալների արտահոսքը (փաստաթղթերը պահի կողավող դարակում, աշխատասենյակից բացակայելիս կամ այլ անձանց ընդունելիս չթողնի անձնական տվյալներ պարունակող փաստաթղթերը տեսանելի վայրում և այլն):

3. Անձնական տվյալների գաղտնիությունը

1) Անձնական տվյալն ինքնին գաղտնիք չէ:

2) Անձնական տվյալները երրորդ անձանց կարող են փոխանցվել կամ այլ կերպ մատչելի դարձվել միայն օրենքներով, այդ թվում՝ «Տեղեկատվության ազատության մասին» Հայաստանի Հանրապետության օրենքով նախատեսված դեպքերում և կարգով:

3) Նախարարության տնօրինության տակ գտնվող անձնական տվյալներին երրորդ անձանց մատչելիությունը կամ այդ տվյալների հանրամատչելիությունը սահմանափակելու անհրաժեշտության դեպքում անձնական տվյալները կամ անձնական տվյալներ պարունակող փաստաթղթերը պետք է դասակարգվեն որպես որևէ գաղտնիք:

4) Նախարարությունը և նախարարության աշխատողները պարտավոր են պահպանել երրորդ անձանց ոչ մատչելի կամ ոչ հանրամատչելի անձնական տվյալների գաղտնիությունը ինչպես անձնական տվյալները մշակելու հետ առնչվող ծառայողական կամ աշխատանքային պարտականությունները կատարելու ընթացքում, այնպես էլ դրա ավարտից հետո:

4. Անձնական տվյալների փոխանցումն այլ պետական մարմիններին

1) Նախարարության տնօրինության տակ գտնվող անձնական տվյալներն այլ պետական մարմիններին կարող են փոխանցվել միայն օրենքներով ուղղակիորեն նախատեսված դեպքերում:

2) Նախարարության տնօրինության տակ գտնվող անձնական տվյալներն օտարերկրյա պետական մարմիններին կարող են փոխանցվել միայն վավերացված միջազգային պայմանագրերի շրջանակներում:

3) Նախարարության տվյալների բազաներում մշակվող անձնական տվյալներն էլեկտրոնային եղանակով փոխանցելու կարգը սահմանվում է ՀՀ կառավարության որոշմամբ:

5. Անձնական տվյալների պաշտպանության համար պատասխանատվություն

1) Անձնական տվյալների պաշտպանության և անվտանգության ապահովման համար նախարարությունը նշանակում է անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձ:

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

3) Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձը՝

ա. ապահովում է «Անձնական տվյալների պաշտպանության մասին» Հայաստանի Հանրապետության օրենքով սահմանված՝ անձնական տվյալներ մշակողի պարտականությունների կատարումը,

բ. ապահովում է նախարարության կապն անձնական տվյալների պաշտպանության լիազոր մարմնի հետ, այդ թվում՝ կազմակերպում անձնական տվյալների մշակման վերաբերյալ խորհրդատվության ստացումը,

գ. կազմում և անձնական տվյալների պաշտպանության լիազոր մարմնի ղեկավարին է ներկայացնում անձնական տվյալների պաշտպանության վերապատրաստման՝ նախարարության ներկայացուցիչների ցուցակը,

դ. ապահովում է անձնական տվյալների պաշտպանության վերաբերյալ քաղաքացիների հարցումների և այլ գրությունների պատասխանները, անհրաժեշտության դեպքում դրանք ներկայացնում անձնական տվյալների պաշտպանության լիազոր մարմնի կարծիքին,

ե. իրականացնում է նախարարության կողմից անձնական տվյալների մշակմանը վերաբերող այլ անհրաժեշտ միջոցառումներ:

4) Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձի հետ կապ հաստատելու տվյալները (էլեկտրոնային փոստի հասցեն, հեռախոսահամարը) տեղադրվում են նախարարության պաշտոնական կայքում:

6. Անձնական տվյալների պաշտպանության իրավունքի վերաբերյալ նախարարության աշխատակիցների վերապատրաստումը

1) Նախարարության՝ անձնական տվյալների մշակման հետ առնչվող աշխատակիցները պետք է անցնեն պարբերական (ոչ պակաս, քան երեք տարին մեկ անգամ) վերապատրաստում անձնական տվյալների պաշտպանության վերաբերյալ:

2) Վերապատրաստումն իրականացվում է անձնական տվյալների լիազոր մարմնի կողմից սահմանված ժամանակացույցով և թեմաներով:

3) Նախարարության նախաձեռնությամբ (առաջարկությամբ) և անձնական տվյալների լիազոր մարմնի համաձայնությամբ կարող են իրականացվել անձնական տվյալների պաշտպանության իրավունքի վերաբերյալ պետական մարմնի համար անհրաժեշտ քանակի և թեմաներով ուսուցումներ: