ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆ
ԱՐՄԱՎԻՐԻ ՄԱՐԶՊԵՏ

ՈՐՈՇՈՒՄ

<< -------->> << ---------- >> 2019թ. **ՆՄՈ/ ----------2019**

ք. Արմավիր

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԱՐՄԱՎԻՐԻ ՄԱՐԶՊԵՏԱՐԱՆԻ ԿՈՂՄԻՑ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ՈՒՂԵՑՈՒՅՑԸ ՀԱՍՏԱՏԵԼՈՒ ՄԱՍԻՆ

Ղեկավարվելով <<Կառավարչական իրավահարաբերությունների կարգավորման մասին>> Հայաստանի Հանրապետության օրենքի 16-րդ հոդվածի 1-ին մասով, <<Անձնական տվյալների պաշտպանության մասին>> Հայաստանի Հանրապետության օրենքի 18-րդ հոդվածով, հիմք ընդունելով Հայաստանի Հանրապետության արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության 2019 թվականի սեպտեմբերի 10-ի թիվ 24/19676-2019 գրությունը.

որոշում եմ՝

1. Հաստատել Հայաստանի Հանրապետության Արմավիրի մարզպետարանի կողմից անձնական տվյալների մշակման ուղեցույցը՝ համաձայն հավելվածի:
2. Սույն որոշումն ուժի մեջ է մտնում ընդունման պահից:

ՄԱՐԶՊԵՏ՝ ***Հ. ՄԱԹԵՎՈՍՅԱՆ***

Invalid signature

X

VERIFIED OCSP 10/1/2019 18:02:50 GMT+4

Signed by: MATEVOSYAN HAMBARDZUM 2809920230

Հավելված
Հայաստանի Հանրապետության Արմավիրի մարզպետի
2019 թվականի -ի
ՈՄՈ/ -2019 որոշման

ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ԱՐՄԱՎԻՐԻ ՄԱՐԶՊԵՏԱՐԱՆԻ ԿՈՂՄԻՑ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ՈՒՂԵՑՈՒՅՑ

Սույն ուղեցույցը նպատակ ունի <<Անձնական տվյալների պաշտպանության մասին>> Հայաստանի Հանրապետության օրենքի դրույթների հիման վրա սահմանել պետական մարմինների կողմից սահմանել 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:

Սույն ուղեցույցում տերմիններն օգտագործվում են նույն իմաստով, ինչ <<Անձնական տվյալների պաշտպանության մասին>> Հայաստանի Հարապետության օրենքում. <<պետական մարմիններ>> եզրույթի շրջանակում նկատի ունենք պետական կառավարման կամ տեղական ինքնակառավարման մարմիններին, պետական կամ համայնքային հիմնարկներին կամ կազմակերպությունների ցանկացած աշխատողի՝ անկախ զբաղեցրած պաշտոնից (հաստիքից), պաշտոնի տեսակից, պայմանագրի տեսակից և այլ առանձնահատկություններից:

1. **Անձնական տվյալներ մշակելու հիմքը, տվյալների մշակում նախատեսելը, տվյալներ ստանալը**
   - ✓ Պետական մարմինների 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:
     - ✓ Այն պարագայում, երբ անհրաժեշտ է, որ պետական մարմինն օգտվի անձնական տվյալի մշակման հանմաձայնության հիմքերից, անհրաժեշտ է, որ այդ հնարավորությունը (հայեցողությունը) նույնպես նախատեսված լինի օրենքով:
     - ✓ Անձնական տվյալների մշակում նախատեսող օրենքներ նախագծելիս, օրենսդրական նախաձեռնություն իրականացնելիս պետական մարմինները պետք է առաջնորդվեն անձնական տվյալների մշակման համաչափության սկզբունքով, այդ թվում.
   - սահմանեն անձնական տվյալների մշակման որոշակի նպատակ,
   - նախատեսեն սահմանված նպատակին հասնելու համար անձնական տվյալների մշակման պիտանի, անհրաժեշտ և չափավոր միջոցներ,
   - նախատեսեն սահմանված նպատակին հասնելու համար անհրաժեշտ նվազագույն քանակի անձնական տվյալների մշակում,
   - չնախատեսեն այնպիսի անձնական տվյալների մշակում, որոնք անհրաժեշտ չեն սահմանված նպատակին հասնելու համար,
   - չնախատեսեն անձնական տվյալների մշակում, եթե սահմանված նպատակին հնարավոր է հասնել ապանձնավորված ձևով,

- նախատեսեն անձնական տվյալների մշակման այնպիսի ժամկետ, որն անհրաժեշտ է սահմանված (այդ թվում՝ արխիվային պահպանության) նպատակին հասնելու համար,
- նախատեսեն կեսաչափական անձնական տվյալների մշակում,եթե սահմանված նպատակը հնարավոր է իրականացնել միայն այդ կենսաչափական տվյալները մշակելու միջոցով:

✓ Պետական մարմինը կարող է ստանալ կամ ձևավորել անձնական տվյալներ միայն օրենքներով ուղղակիորեն սահմանված դեպքում և կարգով:

2. Անձնական տվյալների անվտանգությունը, տվյալների օգտագործումը

✓ Անձնական տվյալների մշակում իրականացնելիս, պետական մարմինը պետք է առաջնորդվի <<Անձնական տվյալների պաշտպանության մասին>> Հայաստանի Հանրապետության օրենքի 5-րդ գլխի դրույթներով:

✓ Պետական մարմինը և պետական մարմնի 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, կրկօրինակումից, տարածումից և այլ միջամտությունից պաշտպանելու համար: Սա վերաբերում է ինչպես պետական մարմնի աշխատողների աշխատանքի կազմակերպմանը, այնպես էլ նրանց կողմից օգտագործվող համակարգչային և այլ տեխնիկական միջոցների պաշտպանվածությանը:

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

✓ Պետական մարմնի 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:

✓ Եթե պետական մարմնի աշխատողին ծառայողական կամ աշխատանքային նպատակներով անձնական տվյալներ պարունակող փաստաթղթեր օգտագործելիս անհրաժեշտ է օգտվել անձնական (ոչ ծառայողական) տեխնիկական միջոցներից (այդ թվում՝ հեռախոս, համակարգիչ և այլն), ապա պետական մարմնի 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:

✓ Եթե պետական մարմնի 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

պետական մարմնի 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:

- ✓ Պետական մարմնի աշխատողը էլեկտրոնային փաստաթղթաշրջանառության համակարգից (օրինակ՝ <<Mulberry>> համակարգ) օգտվելիս պետք է սահմանափակվի այլ աշխատողների հասանելիությունը ծառայողական կամ աշխատանքային նպատակներով իրեն վստահված կամ հայտնի դարձած և ոչ հանրամատչելի 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:
- ✓ Պետական մարմնի 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 փաստաշրջանառության համակարգի (օրինակ՝ <<Mulberry>> համակարգի) իր անձնական էջ մուտք գործելու տվյալները՝ մուտքանունը և գաղտնաբառը:
- ✓ Պետական մարմնի աշխատողի՝ աշխատանքից ազատվելու պարագայում անհրաժեշտ է արգելափակել տվյալ անձի էլեկտրոնային փաստաշրջանառության համակարգի անձնական էջը՝ նրա կողմից այլ տեխնիկական սարքավորումներից և անձնական նպատակներով համակարգ մուտք գործելը կանխելու համար:
- ✓ Վերոնշյալ կանոնները վերաբերվում են նյութական կրիչով (ներառյալ թղթային տարբերակով) կամ էլեկտրոնային փոստի միջոցով ծառայողական կամ աշխատանքային նպատակներով պետական մարմնի աշխատողին վստահված կամ հայտնի դարձած և ոչ հանրամատչելի անձնական տվյալների հասանելության սահմանափակմանը՝ նյութական կրիչի կամ էլեկտրոնային փոստի մատչելիությանը վերաբերել իմիջոցներով: Մասնավորապես, պետական մարմնի 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 (աշխատասեղանին) պահի այնպես, որ կանխվի անձնական տվյալների արտահոսքը (փաստաթղթերը պահի կողպվող դարակում, աշխատասենյակից բացակայելիս կամ այլ անձանց ընդունելիս չթողնի անձնական տվյալներ պարունակող փաստաթղթերը տեսանելի վայրում և այլն):

3. Անձնական տվյալների գաղտնիությունը

- ✓ Անձնական տվյալն ինքնին գաղտնիք չէ:
- ✓ 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:

- ✓ Պետական մարմնի 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:
- ✓ Պետական մարմինը և պետական մարմնի աշխատողները պարտավոր են պահպանել երրորդ անձանց ոչ մատչելի կամ ոչ հանրամատչելի անձնական տվյալների գաղտնիությունը ինչպես անձնական տվյալներ մշակելու հետ առնչվող ծառայողական կամ աշխատանքային պարտականությունները կատարելու ընթացքում, այնպես էլ դրա ավարտից հետո:

4. Անձնական տվյալների փոխանցումն այլ պետական մարմիններին

- ✓ Պետական մարմնի տնօրինության տակ գտնվող անձնական տվյալներն այլ պետական մարմիններին կարող են փոխանցվել միայն օրենքներով ուղղակիորեն նախատեսված դեպքերում:
- ✓ Պետական մարմինների տնօրինության տակ գտնվող անձնական տվյալներն օտարերկրյա պետական մարմիններին կարող են փոխանցվել միայն վավերացված միջազգային պայմանագրերի շրջանակներում:
- ✓ Պետական մարմինների տվյալների բազաներում մշակվող անձնական տվյալներն էլեկտրոնային եղանակով փոխանցելու կարգը սահմանվում է ՀՀ կառավարության որոշմամբ:

5. Անձնական տվյալների պաշտպանության համար պատասխանատուն

- ✓ Անձնական տվյալների պաշտպանության և անվտանգության ապահովման համար պետական մարմինը նշանակում է անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձ:
- ✓ Անձնական տվյալների պաշտպանության համար պատասխանատու պաշտոնատար անձ չնշանակելու դեպքում անձնական տվյալների պաշտպանության համար պատասխանատու է պետական մարմնի ղեկավարը կամ գլխավոր քարտուղարը՝ կախված տվյալների մշակման դեպքից:
- ✓ 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՝ պետական մարմնի 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:

6. Անձնական տվյալների պաշտպանության իրավունքի վերաբերյալ պետական մարմինների աշխատակիցների վերապատրաստումը

- ✓ Պետական մարմնի՝ անձնական տվյալների մշակման հետ առնչվող աշխատակիցները պետք է անցնեն պարբերական (ոչ պակաս, քան երեք տարին մեկ անգամ) վերապատրաստում անձնական տվյալների պաշտպանության վերաբերյալ:
- ✓ Վերապատրաստումն իրականացվում է անձնական տվյալների լիազոր մարմնի կողմից սահմանված ժամանակացույցով և թեմաներով:
- ✓ Պետական մարմնի նախաձեռնությամբ (առաջարկությամբ) և անձնական տվյալների լիազոր մարմնի համաձայնությամբ կարող են իրականացվել անձնական տվյալների պաշտպանության իրավունքի վերաբերյալ պետական մարմնի համար անհրաժեշտ քանակի և թեմաներով ուսուցումներ:

Գլխավոր քարտուղարի պաշտոնակատար՝ **Վ. Վարդազարյան**

Недействительная подпись

X

VERIFIED OCSP 01.10.2019 17:58:25 GMT+4

Подписано: VARDAZARYAN VARDAN 1704780217