ՀՀ ԱՐԴԱՐԱԴԱՏՈՒԹՅԱՆ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

unicef

Զգու՛յշ, երեխաներ են

ուղեցույց երեխաների անձնական տվյալների պաշտպանության վերաբերյալ երեխաների եւ բոլորի համար

ԵՐԵՎԱՆ, 2018

Կազմի նկարագիրը և հեղինակային իրավունքը՝
Ք. Երևան, Մալաթիա-Սեբաստիա վարչական
շրջանում գտնվող թիվ 92 մանկապարտեզում
© UNICEF/Armenia 2018/Osipova

Հայաստանի Հանրապետության
Արդարադատության նախարարություն

unicef
յուրաքանչյուր երեխայի համար

Զգու՛յշ, երեխաներ են

ուղեցույց երեխաների անձնական տվյալների պաշտպանության վերաբերյալ երեխաների եւ բոլորի համար

ՀՀ ԱՐԴԱՐԱԴԱՏՈՒԹՅԱՆ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԳՈՐԾԱԿԱԼՈՒԹՅՈՒՆ

ԵՐԵՎԱՆ, 2018

Սույն ուղեցույցը կազմվել է 2018 թվականին ՅՈՒՆԻՍԵՖ-ի (ՄԱԿ-ի մանկական հիմնադրամի) աջակցությամբ իրականացվող «Բազմաոլորտային ազգային հարթակի ուժեղացում՝ ուղղված երեխաների հանդեպ բռնությանը վերջ դնելու գործողությունների պլանավորմանը, իրագործմանը և գնահատմանը» ծրագրի շրջանակում, որն իրականացվել է «Իրավական կրթության և վերականգնողական ծրագրերի իրականացման կենտրոն» ՊՈԱԿ-ի կողմից: Արտահայտված տեսակետները պարտադիր չէ, որ արտահայտեն ՅՈՒՆԻՍԵՖ-ի տեսակետները և քաղաքականությունը:

Հեղինակներ՝

Գևորգ Հայրապետյան
ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության պետ

Մկրտիչ Խաչատրյան
ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության փորձագետ

Սրբագրման և տպագրման աշխատանքներ՝

Անահիտ Խաչատրյան
«Իրավական կրթության և վերականգնողական ծրագրերի իրականացման կենտրոն» ՊՈԱԿ-ի առաջատար մասնագետ

Սամվել Աբրահամյան
«Իրավական կրթության և վերականգնողական ծրագրերի իրականացման կենտրոն» ՊՈԱԿ-ի գլխավոր մասնագետ

Պատասխանատու՝

Գայանե Հովակիմյան
«Իրավական կրթության և վերականգնողական ծրագրերի իրականացման կենտրոն» ՊՈԱԿ-ի վերականգնողական ծրագրերի իրականացման հարցերով տնօրենի տեղակալ, Անչափահասների արդարադատության խորհրդի քարտուղար

«Իրավական կրթության և վերականգնողական
ծրագրերի իրականացման կենտրոն» ՊՈԱԿ
ք. Երևան, Մովսես Խորենացի 162ա
հեռ. +37410 574 406
էլ.փոստ: info@lawinstitute.am

Բովանդակություն

Նախաբան 4

Անձնական տվյալների պաշտպանության
հիմնական հասկացությունները 7

Անձնական տվյալների տեսակները..... 16

Անձնական տվյալների մշակման սկզբունքները 24

Թեստեր 31

Նախաբան

Անձնական տվյալների պաշտպանության իրավունքը մարդու հիմնական իրավունքներից է. չէ՞ որ յուրաքանչյուրը պետք է ունենա հնարավորություն պաշտպանելու իրեն վերաբերող տվյալները, թույլ չտալու, որ իր, իր կյանքի, իր առօրյայի եւ իրեն վերաբերող ցանկացած տեղեկություն օգտագործվի ապօրինի կերպով եւ անհանգստացնի իրեն:

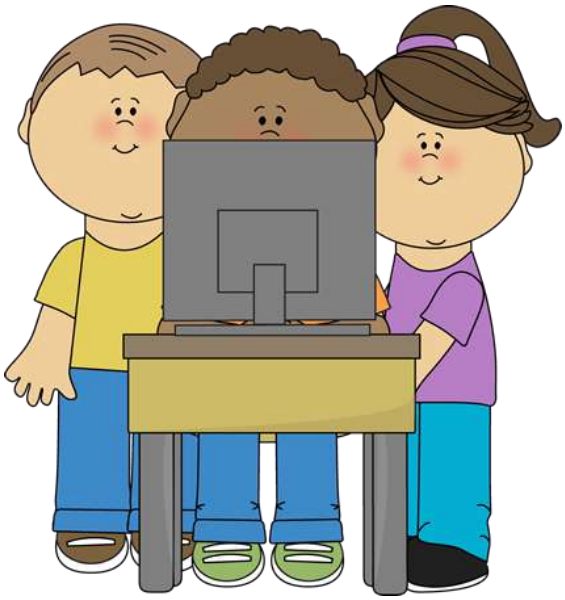
Պատահական չէ, որ Հայաստանի Սահմանադրությամբ ամրագրված այս իրավունքն առարկայացնելու համար 2015 թվականին ընդունվեց «Անձնական տվյալների պաշտպանության մասին» օրենքը՝ սահմանելով այն կանոնները, որոնք պետք է պահպանել մարդու վերաբերյալ տվյալների հետ առնչվելիս: **Օրենքի հիման վրա կրկին 2015 թվականին ստեղծվեց նաև ՀՀ արդարադատության նախարարության կազմում գործող Անձնական տվյալների պաշտպանության գործակալությունը, որի նպատակն է իրականացնել մարդկանց անձնական տվյալների պաշտպանությունը:**

Գործակալության գործունեության առաջին տարիների ընթացքում պարզ դարձավ, որ անձնական տվյալների պաշտպանության ոլորտում ամենակարեւոր խնդիրներից է երեխաների անձնական տվյալների պաշտ-պանությունը: Երեխաների անձնական տվյալների պաշտպանությունն ունի իր առանձնահատկությունը. բանն այն է, որ երեխաներն իրենց փոքր տարիքի հետեւանքով, երբ դեռ գտնվում են ֆիզիկական եւ մտավոր զարգացման, իրավագիտակցության ձեւավորման ճանապարհին, կարող են ամբողջությամբ չգիտակցել իրենց անձնական տվյալների պաշտպանության կարեւորությունը կամ գիտակցեն, բայց չկարողանան պատշաճ կերպով իրականացնել իրենց իրավունքի պաշտպանությունը: Ուստի, երեխաներն, ի տարբերություն չափահասների, լրացուցիչ օժանդակության եւ ավելի շատ պաշտպանության կարիք ունեն իրենց իրավունքների պաշտպանության հարցում:

Նաեւ, Գործակալությունը հանդիպեց բազմաթիվ դեպքերի, երբ երեխաների անձնական տվյալներն անհարկի վտանգվել էին: Արդյունքում, նախ Գործակալությունը հրապարակեց խորհրդատվական որոշում երեխաների

անձնական տվյալների հրապարակման վերաբերյալ[1], ապա հրապարակեց նաեւ ավելի ամբողջական ուղեցույց երեխաների անձնական տվյալների պաշտպանության մասին[2]: Ուղեցույցը ներկայացնում էր երեխաների անձնական տվյալների պաշտպանության սկզբունքները, անձնական տվյալների պաշտպանության ոլորտում երեխաների իրավունքները և տվյալներ մշակողների պարտականություններն ու պատասխանատվությունը, ներկայացնում էր օրենսդրական կարգավորումները՝ հիմնականում կիրառելով նաեւ իրավաբանական տերմինաբանություն:

Անձնական տվյալների պաշտպանության գործակալության կողմից մշակված այս ուղեցույցը նպատակ ունի լրացնել Գործակալության կողմից մշակված նախորդ ուղեցույցն ավելի պրակտիկ խորհուրդներով, երեխաների անձնական տվյալների պաշտպանության կանոնները ներկայացնել առավել հանրամատչելի ձեւով, պատկերավոր օրինակներով, թեստերով եւ խնդիրներով եւ ուղղված է ոչ միայն



երեխաների ծնողներին, երեխայի խնամքով կամ կրթությամբ զբաղվող մասնագիտացված կառույցների եւ հաստատությունների աշխատակիցներին, այլ նաեւ՝ հենց երեխաներին: Թեեւ այս ուղեցույցը մշակվել եւ հրապարակվել է երեխաների անձնական տվյալների պաշտպանության վերաբերյալ նախորդ ուղեցույցից հետո, սակայն այն իր կառուցվածքի եւ բովանդակության տրամաբանությամբ նախորդում է վերջինիս, քանի որ տալիս է հիմնական գիտելիքներ անձնական տվյալների պաշտպանության մասին, պարզ՝ ոչ իրավաբանական լեզվով, սովորեցնում կողմնորոշվել, թե ինչ է անձնական տվյալը, ինչպիսի տեսակներ կան եւ ինչպես է պետք վարվել դրանց հետ: Ուստի, խորհուրդ կտանք նախ ծանոթանալ այս ուղեցույցին, ապա, իրավական գիտելիքներն ավելի խորացնելու անհրաժեշտության դեպքում ուսումնասիրել նաեւ երեխաների անձնական տվյալների պաշտպանության վերաբերյալ Գործակալության նախորդ ուղեցույցը, ապա նաեւ՝ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքը:

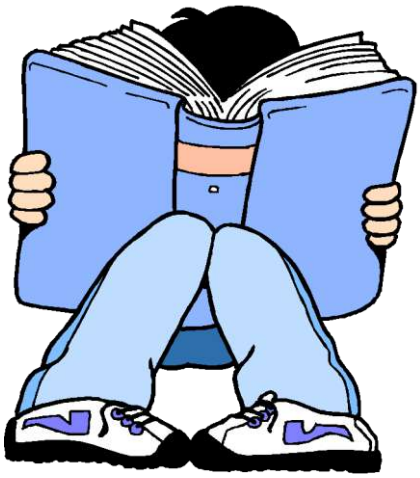
---

[1] Խորհրդատվական որոշումը հասանելի է ՀՀ արդարադատության նախարարության www.moj.am կայքում, «Գրադարան» բաժնի «Անձնական տվյալների պաշտպանության գործակալության որոշումները» ենթաբաժնում:

[2] Ուղեցույցը հասանելի է ՀՀ արդարադատության նախարարության www.moj.am կայքում, «Գրադարան» բաժնի «Անձնական տվյալների պաշտպանության գործակալության որոշումները» ենթաբաժնում:

Ուղեցույցը մշակվել է այնպես եւ նաեւ այն նպատակով, որ կարողանա ծառայել որպես ուսումնական ձեռնարկ՝ երեխաներին իրենց անձնական տվյալների պաշտպանության իրավունքին ծանոթացնելու, անձնական տվյալների նկատմամբ ուշադրությունը բարձրացնելու, ինչպես նաեւ իրենց վերաբերյալ տվյալների պաշտպանությունն ինքնուրույն իրականացնել սովորեցնելու համար:

Ուղեցույցը մշակվել է անձնական տվյալների պաշտպանության օրենսդրության, Անձնական տվյալների պաշտպանության գործակալության կողմից իրականացվող ուսուցողական նյութերի, ինչպես նաեւ անձնական տվյալների պաշտպանության իրավունքի վերաբերյալ գիտագործնական մեկնաբանությունների հիման վրա:



Երեխաների անձնական տվյալների պաշտպանությունն ունի իր առանձնահատկությունները, ինչը պայմանավորված է երեխաների կարգավիճակով, սակայն հիմնական հասկացությունները, տվյալների մշակման սկզբունքները եւ կանոնները նույնն են: Ուստի, սկսենք ծանոթացնել անձնական տվյալների պաշտպանության իրավունքին:

Անձնական տվյալների պաշտպանության հիմնական հասկացությունները

Ուղեցույցի այս բաժնում կներկայացնենք անձնական տվյալների պաշտպանության ոլորտում կիրառվող հիմնական հասկացությունները, կներկայացնենք, թե ինչպես պետք է որոշել՝ այս կամ այն տեղեկությունն անձնական տվյալ է, թե ոչ: Պատկերավոր ասած՝ այս բաժինն անձնական տվյալների պաշտպանության իրավունքի բացատրական բառարանն է:

- Այսպես, նախաբանում բազմիցս նշեցինք անձնական տվյալների մասին. բայց ի վերջո՝ ի՞նչ է անձնական տվյալը, ո՞ր տեղեկություններն են, որ համարվում են անձնական տվյալներ:

Անձնական տվյալի հասկացությունը հետեւյալն է՝ **անձնական տվյալ՝** ֆիզիկական անձին վերաբերող ցանկացած տեղեկություն, որը թույլ է տալիս կամ կարող է թույլ տալ ուղղակի կամ անուղղակի կերպով նույնականացնել անձի ինքնությունը (օրինակ՝ անուն, ազգանուն, նույնականացման քարտի համար, հեռախոսահամար, նկար, բնակության հասցե, տարիք և այլն):

Այսպես, անձնական տվյալ է այն տեղեկությունը, որը վերաբերում է **ֆիզիկական անձին:** Անձնական տվյալների պաշտպանության ոլորտում կարող եք հանդիպել նաեւ այլ արտահայտությունների, օրինակ, որ անձնական տվյալներն **անձինն** են կամ **անհատինը,** կամ **քաղաքացունը,** կամ որ անձնական տվյալների պաշտպանության իրավունք ունի **յուրաքանչյուր ոք:** Այս բոլոր արտահայտությունները վերաբերում են **մարդուն՝** այսինքն, **մարդուն վերաբերող տվյալներն են, որ համարվում են անձնական:**

Ինչպես երեւում է անձնական տվյալների հասկացությունից՝ անձնական տվյալները կարող են լինել այնպիսին, որ **թույլ են տալիս ուղղակիորեն նույնականացնել** մարդուն. օրինակ՝ մարդու լուսանկարը: Այսպես, եթե ունեք մարդու լուսանկարը, որն այլ մարդկանց հետ միասին գտնվում է սենյակում, ապա առանց որեւէ հավելյալ տվյալների, միայն լուսանկարն ունենալով, կարող եք սենյակում գտնել եւ ճանաչել լուսանկարում պատկերված մարդուն: Ուրեմն,

մարդու լուսանկարն անձնական տվյալ է: Չմոռանանք նաեւ մարդուն ճանաչելու, նրա հետ ծանոթանալու համար ամենատարածված տվյալները՝ մարդու անունը եւ ազգանունը:

Անձնական տվյալները կարող են լինել նաև այնպիսին, որ **կարող են թույլ տալ անուղղակիորեն նույնականացնել մարդուն:** Այս դեպքում անձնական տվյալն անհրաժեշտ կլինի համադրել այլ տեղեկությունների հետ նույնպես: Օրինակ, եթե վերցնեք որեւէ մեկի բջջային հեռախոսահամարը կամ տեսնեք մեքենայի համարանիշը, ապա դա դեռ բավական չի լինի, որ միանգամից հասկանաք, թե ում են պատկանում դրանք. անհրաժեշտ կլինեն նաեւ այլ տեղեկություններ. ասենք, մարդու անուն ազգանունը, բնակության հասցեն եւ այլն: Նման կերպ է վարվում Ճանապարհային ոստիկանությունը, երբ փողոցներում տեղադրված տեսախցիկներով խախտում է հայտնաբերում. չէ՞ որ սկզբում Ճանապարհային ոստիկանությունն ունենում է միայն տեսախցիկի տեսագրության կամ արագաչափ սարքի լուսանկարի մեջ պատկերված համարանիշը, այդուհետ այդ համարանիշը համադրում է մեքենայի մակնիշի հետ եւ գտնում այդ մեքենայի սեփականատիրոջը, որպեսզի տուգանի կատարած խախտման համար: Այս դեպքում մարդուն տրամադրված համարանիշն այն տվյալն էր, որը թույլ տվեց անուղղակիորեն, այլ տվյալների հետ համադրելով, գտնել եւ նույնականացնել մեքենայի սեփականատիրոջը: Ուրեմն, մարդուն տրամադրված համարանիշն անձնական տվյալ է:

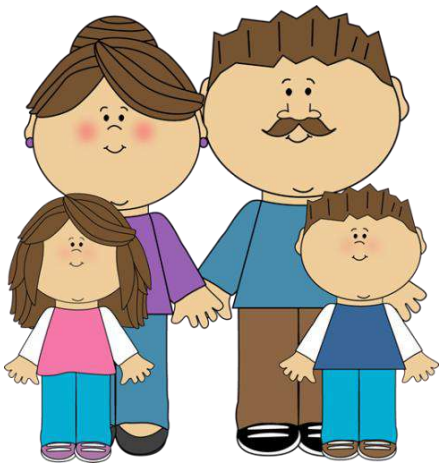
- *Հիշու՞մ եք՝ անձնական են այն տվյալները, որոնք վերաբերում են մարդուն: Սա նշանակում է, որ մեքենայի համարանիշը կամ բջջային հեռախոսահամարը, որոնք դեռ որեւէ մեկին չեն տրամադրվել, այլ դրված են ճանապարհային ոստիկանությունում կամ բջջային օպերատորի մոտ, դեռեւս անձնական տվյալներ չեն: Դրանք դառնում են անձնական տվյալներ, երբ տրամադրվում են որեւէ մարդու եւ սկսում են վերաբերել այդ մարդուն:*

- Այն անձը, ում վերաբերում են անձնական տվյալները, կոչվում է **տվյալների սուբյեկտ:**

Տվյալների սուբյեկտ արտահայտությունն առավել հաճախ հանդիպում է «Անձնական տվյալների պաշտպանության մասին» օրենքում, ինչպես նաեւ այլ օրենքներում, այլ իրավական ակտերում: Ամեն դեպքում հիշեք՝ տվյալների սուբյեկտն այն մարդն է, ում վերաբերում են անձնական տվյալները. այս արտահայտությունը հնարավոր է օգտագործենք նաեւ այս ուղեցույցում:

- *Այս համատեքստում պետք է նկատի ունենալ, որ երեխայի անձնական տվյալների սուբյեկտը հենց երեխան է, այլ ոչ ծնողը կամ օրինական ներկայացուցիչը՝ անկախ երեխայի տարիքից, անկախ ֆիզիկական եւ մտավոր զարգացվածությունից եւ անկախ իրավագիտակցության մակարդակից: Ընդ որում, պետք է հաշվի առնել, որ թեեւ երեխա է համարվում տասնութ տարին չլրացած անձը (18 տարին լրանալու դեպքում անձը դադարում է երեխա համարվելուց և դուրս է գալիս ծնողական խնամքից), սակայն, անձնական տվյալների պաշտպանության ոլորտում 16 տարին լրացած երեխան անձնական տվյալների պաշտպանության իրավունքով սահմանված իր իրավունքներն անձամբ է իրականացնում եւ կարող է ամբողջությամբ ինքնուրույն կայացնել իր անձնական տվյալների մշակման վերաբերյալ որոշումներ: Հետեւաբար, այս ուղեցույցում ասելով երեխա՝ նկատի ունենք տասնվեց տարին չլրացած անձանց:*

- Հաճախ հանդիպող տերմիններից է նաեւ **անձնական տվյալների մշակումը,** որի հասկացությունը հետեւյալն է՝ անկախ իրականացման ձեւից եւ եղանակից (այդ թվում՝ ավտոմատացված, տեխնիկական ցանկացած միջոցներ կիրառելու կամ առանց դրանց) ցանկացած գործողություն կամ գործողությունների խումբ, որը կապված է անձնական տվյալները հավաքելու կամ ամրագրելու, կամ մուտքագրելու, կամ համակարգելու, կամ կազմակերպելու, կամ պահպանելու կամ օգտագործելու կամ վերափոխելու, կամ վերականգնելու, կամ փոխանցելու կամ ուղղելու կամ ուղեփակելու կամ ոչնչացնելու կամ այլ գործողություններ կատարելու հետ:



Իսկապես, անձնական տվյալների հետ կարելի է բազմաթիվ գործողություններ անել՝ անձնական տվյալները հավաքել, օրինակ՝ մարդկանց լուսանկարելու միջոցով, կամ փոխանցել. օրինակ, երբ ընկերոջ հեռախոսահամարը եւ անունը տրամադրում եք մեկ ուրիշ ընկերոջ, կամ ամրագրել եւ պահպանել, օրինակ, երբ

գրանցում եք նոր ծանոթի կոնտակտային տվյալները եւ անունն ու ազգանունը հեռախոսագրքում եւ այլն: Անձնական տվյալների հետ իրականացվող գործողությունները բազմաթիվ են, անգամ հասկացության մեջ դրանք սպառիչ չեն թվարկված (նշված է՝ **եւ այլ գործողություններ**), ուստի անձնական տվյալների հետ հնարավոր կատարվելիք բոլոր գործողությունները մեկ բառով բնութագրվում է որպես **մշակում**: Այսուհետ ուղեցույցում էլ անձնական տվյալների հետ կատարվող բազմաթիվ գործողությունները հատ-հատ թվարկելու փոխարեն երբեմն կօգտագործենք **անձնական տվյալների մշակում** արտահայտությունը:

Անձնական տվյալների հետ կատարվող գործողություններն էլ (անձնական տվյալների մշակումը) կարելի է իրականացնել տարբեր ձեւերով. օրինակ՝ ընկերոջ հեռախոսահամարը եւ անունը մեկ ուրիշ ընկերոջը փոխանցել հնարավոր է էլեկտրոնային փոստի միջոցով, կամ, օրինակ, Ֆեյսբուքի հաղորդագրության միջոցով գրելով կամ հեռախոսով բանավոր հայտնելով: Կարելի է նաեւ ծանոթի կոնտակտային տվյալները եւ անունն ու ազգանունը գրանցել եւ պահպանել նոթատետրում, կամ հեռախոսագրքում կամ համակարգչի մեջ: Ինչպես տեսնում եք, տվյալների մշակման ձեւերը նույնպես տարբեր են:

- *Հիշեք, անձնական տվյալների հետ կատարվող ցանկացած գործողությունը համարվում է մշակում՝ անկախ գործողության իրականացման ձեւից:*

- *Կարեւոր է նկատի ունենալ, որ անձնական տվյալները հրապարակելը (այդ թվում՝ սոցիալական ցանցերով կամ առհասարակ համացանցով կամ լրատվամիջոցներով), այլ անձանց մատչելի դարձնելը, այլ անձանց փոխանցելը կամ այդ տվյալների ծանոթացնելը նույնպես համարվում է անձնական տվյալների մշակում:*

- Անձնական տվյալների պաշտպանության ոլորտում բավական հաճախ է հանդիպում **անձնական տվյալներ մշակող** հասկացությունը: Արդեն քննարկեցինք, թե ինչ է անձնական տվյալը, ինչն է համարվում անձնական տվյալի մշակում եւ ով է անձնական տվյալի սուբյեկտը: Անձնական տվյալներ մշակողի հասկացությունը վերջինն է անձնական տվյալների պաշտպանության ոլորտի այն կարեւոր տերմիններից, որը կքննարկենք այս ուղեցույցում:

Հասկացությունը հետեւյալն է. **Անձնական տվյալներ մշակող՝** պետական կառավարման կամ տեղական ինքնակառավարման մարմին, պետական կամ համայնքային հիմնարկ կամ կազմակերպություն, իրավաբանական կամ ֆիզիկական անձ, որը կազմակերպում և (կամ) իրականացնում է անձնական տվյալների մշակում:

- *Հիշու՞մ եք՝ սկզբում նշեցինք, որ **ֆիզիկական անձ** ասելիս պետք է նկատի ունենալ **մարդուն:** Անձնական տվյալներ մշակողի հասկացության մեջ նշված է նաեւ իրավաբանական անձանց մասին (իրավաբանական եւ ֆիզիկական անձ): Այսպես, իրավաբանական անձինք կազմակերպություններն են. որպես կանոն՝ մասնավոր կազմակերպությունները. Օրինակ՝ սահմանափակ պատասխանատվությամբ ընկերությունները (ՍՊԸ), փակ բաժնետիրական ընկերությունները կամ բաց բաժնետիրական ընկերությունները (ՓԲԸ կամ ԲԲԸ), հասարակական կազմակերպությունները (ՀԿ), հիմնադրամները եւ այլն:*

Այսպես, անձնական տվյալներ մշակող կարող են լինել **բոլորը՝** ե՛ւ մարդիկ, ե՛ւ մասնավոր կազմակերպությունները, ե՛ւ պետական մարմինները (օրինակ՝ նախարարությունները, կառավարությունը եւ այլն), ե՛ւ տեղական ինքնակառավարման մարմինները (քաղաքապետարանները եւ գյուղապետարանները): Անձնական տվյալներ մշակող համարվելու միակ չափանիշն այն է, որ մշակողը պետք է կամ **իրականացնի** կամ **կազմակերպի** անձնական տվյալների մշակում:

- *Հիշու՞մ եք՝ անձնական տվյալների մշակումն անձնական տվյալի հետ կատարվող գործողությունն է: Հետեւաբար, անձնական տվյալների մշակող է համարվում նա, ով մարդու վերաբերյալ տվյալների հետ իրականացնում է որեւէ գործողություն կամ կազմակերպում է այդ գործողության իրականացումը:*

Ինչպես տեսնում եք, անձնական տվյալներ մշակող է համարվում ոչ միայն անձնական տվյալներ մշակում իրականացնողը, այլ նաեւ՝ կազմակերպողը: Օրինակ՝ հաճախ է լինում, որ սոցիալական հարցում անցկացնելու նպատակով այցելում են մարդկանց տներ եւ այդ նպատակով վերցնում նաեւ անձնական տվյալներ՝ անուն, ազգանուն, անձնագրային տվյալներ, ընտանիքի անդամների թիվը եւ այլն:

Որոշ դեպքերում սոցիալական հարցում իրականացնող կազմակերպությունը դա անում է հենց իր համար, իր կարիքների կամ վերլուծությունների համար եւ անձնական տվյալներն էլ վերցնում է համապատասխանաբար իր նպատակին հասնելու համար: Այս դեպքում անձնական տվյալներ մշակողը հենց սոցիալական հարցում իրականացնողն է, որը սոցիալական հարցման նպատակով իրականացնում է անձնական տվյալների մշակում (հավաքում է անձնական տվյալները, վերլուծում եւ այլն):

Որոշ դեպքերում էլ սոցիալական հարցում իրականացնող կազմակերպությունը դա անում է այլ կազմակերպության պատվերով՝ այլ կազմակերպության համար, եւ անձնական տվյալներն էլ վերցնում է ոչ թե իր, այլ սոցիալական հարցումը պատվիրած կազմակերպությանը փոխանցելու համար: Այս դեպքում անձնական տվյալներ մշակողը ոչ թե սոցիալական հարցում իրականացնողն է, այլ այն կազմակերպությունը, որը պատվիրել է սոցիալական հարցումը: Սոցիալական հարցումը պատվիրող կազմակերպությունն այս դեպքում թեեւ ինքնուրույն չի հավաքում անձնական տվյալներ, սակայն համարվում է անձնական տվյալներ մշակող, քանի որ կազմակերպում է դրանց մշակումը:

- *Անձնական տվյալներ մշակողին ճիշտ պարզելու համար հարց տվեք՝ ո՞վ է սահմանում անձնական տվյալների մշակման նպատակը եւ պայմանները, ում համար են մշակվում անձնական տվյալները եւ ով է որոշում, թե ինչ անձնական տվյալներ եւ ինչպես պետք է մշակվեն. նման որոշումներ կայացնողն էլ հենց կոնկրետ դեպքում կհամարվի անձնական տվյալներ մշակող, իսկ մշակողի անունից եւ մշակողի հանձնարարությամբ տվյալների մշակում փաստացի կատարողը կհամարվի տվյալներ մշակողի լիազորված անձ:*

- *Վերոնշյալի համատեքստում պետք է նկատի ունենալ, որ երեխաների անձնական տվյալներ մշակող է համարվում յուրաքանչյուրը, ով որեւէ կերպ օգտագործում է երեխայի վերաբերյալ տեղեկությունները, այդ թվում՝ ուսումնական հաստատությունները՝ մանկապարտեզները, դպրոցները եւ այլն: Անգամ ծնողները կհամարվեն տվյալներ մշակող, եթե իրենց երեխաների անձնական տվյալներն օգտագործեն ոչ թե երեխայի անունից, այլ իրենց համար, օրինակ, համացանցում իրենց էջերում երեխաների լուսանկարը հրապարակելու դեպքում:*

Գործնական օրինակ.

Նկար 1

Նկար 1-ում Մկրտիչ Խաչատրյանն է՝ Անձնական տվյալների պաշտպանության գործակալության փորձագետը (ինչպես նշել ենք նախաբանում՝ Անձնական տվյալների պաշտպանության գործակալությունն այն պետական մարմինն է, որն իրականացնում է անձնական տվյալների պաշտպանությունը):

Այս նկարով պարզապես նպատակ ունենք ծանոթացնել Մկրտիչի հետ: Այժմ արդեն գիտեք, թե Մկրտիչի արտաքինը, այդ թվում՝ թե նա հագուստի ինչ ոճ ունի:

Նկար 2

Նկար 2-ում արդեն երկու անձ է պատկերված՝ Մկրտիչ Խաչատրյանը, ինչպես նաեւ Անձնական տվյալների պաշտպանության գործակալության պետը՝ Գեւորգ Հայրապետյանը: Ունենալով նկար 1-ը՝ դժվար չէ միանգամից հասկանալ, թե նկար 2-ում պատկերված անձանցից ո՞րն է Մկրտիչը, ճանաչել եւ նույնականացնել նրան: Հետեւաբար, նկար 1-ը հնարավորություն տվեց նկար 2-ում միանգամից նույնականացնել Անձնական տվյալների պաշտպանության գործակալության փորձագետին: Այսպես, նկար 1-ը պարունակում է անձնական տվյալ, այն է՝ Մկրտիչ Խաչատրյանի պատկերը: Նմանապես, նկար 2-ը նույնպես պարունակում է անձնական տվյալներ, այս անգամ ե՛ւ Մկրտիչ Խաչատրյանինը, ե՛ւ Գեւորգ Հայրապետյանինը:

Նույն նկարների օգնությամբ անդրադառնանք նաեւ տվյալների սուբյեկտ հասկացությանը: Այսպես, նկար 1-ում միայն Մկրտիչ Խաչատրյանն է պատկերված, նկար 1-ը վերաբերում է միայն Մկրտիչ Խաչատրյանին, հետեւաբար այս դեպքում տվյալների սուբյեկտը միայն նա է: Իսկ նկար 2-ը պատկերում է երկու անձանց եւ վերաբերում է ինչպես Մկրտիչ Խաչատրյանին, այնպես էլ Գեւորգ Հայրապետյանին: Ուստի, նկար 2-ի դեպքում տվյալների սուբյեկտները երկուսն են՝ Մկրտիչ Խաչատրյանը և Գեւորգ Հայրապետյանը:

Քննարկենք նաև նկար 1-ը եւ նկար 2-ն այս ուղեցույցում ներառելու դեպքում կա՞ արդյոք անձնական տվյալների մշակում: Այսպես, այս ուղեցույցով նկար 1-ի եւ նկար 2-ի միջոցով հրապարակվել են Մկրտիչ Խաչատրյանի եւ Գեւորգ Հայրապետյանի պատկերները, բացի այդ, նրանց նկարներն օգտագործվել են որպես օրինակներ: Քանի որ ինչպես անձնական տվյալների հրապարակումը, այնպես էլ օգտագործումը անձնական տվյալների հետ իրականացվող գործողություններ են, ապա այս դեպքում առկա է անձնական տվյալների մշակում. Մկրտիչ Խաչատրյանի եւ Գեւորգ Հայրապետյանի նկարների հրապարակմամբ նրանց անձնական տվյալները մշակվել են:

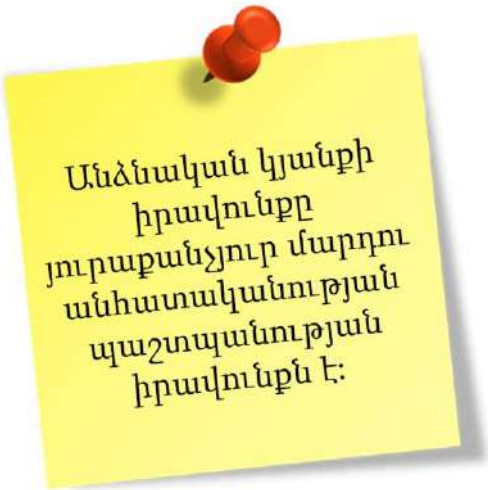
Եւ վերջում պարզենք, թե ով է մշակողը: Ինչպես նշեցինք նախաբանում, այս ուղեցույցը պատրաստել է Անձնական տվյալների պաշտպանության

գործակալությունը: Գործակալությունն ուղեցույցը պատրաստել է օրենքով իրեն տրված լիազորությունների շրջանակներում անձնական տվյալների պաշտպանության նպատակն իրականացնելու համար: Նաեւ, Գործակալությունն է որոշել, որ ուղեցույցի նպատակներին հասնելու համար (տվյալ դեպքում՝ անձնական տվյալների հասկացությունները օրինակներով ամրապնդելու համար) անհրաժեշտ է ուղեցույցում ներառել մարդկանց պատկերով նկարներ եւ նկարներում պատկերված անձանց համաձայնությամբ (համաձայնության անհրաժեշտության մասին կխոսենք հաջորդիվ՝ ուղեցույցի 3-րդ բաժնում) հենց Գործակալությունն է նկար 1-ը եւ նկար 2-ը հրապարակել ուղեցույցում: Տվյալ դեպքում, Անձնական տվյալների պաշտպանության գործակալությունն է անձնական տվյալներ մշակողը՝ անկախ նրանից, թե ով է սրբագրել այս ուղեցույցը, ով է իրականացրել ուղեցույցի ձեւավորումը կամ ով է տպագրել ուղեցույցը:

Անձնական տվյալների տեսակները

Ուղեցույցի այս բաժնում, կներկայացնենք անձնական տվյալների տեսակները եւ կբացատրենք դրանք տարանջատելու իմաստը: Այո, տարբեր անձնական տվյալներ են լինում. դրանք բաժանվում են տեսակների՝ ըստ այնպիսի չափանիշների, որոնք ընդհանուր եւ բնորոշ են անձնական տվյալների մի խմբի համար:

- Այսպես, նախ ներկայացնենք **անձնական կյանքի տվյալները.** անձնական կյանքի տվյալներ են մարդու անձնական կյանքի, ընտանեկան կյանքի, ֆիզիկական, ֆիզիոլոգիական, մտավոր, սոցիալական վիճակի վերաբերյալ կամ նման այլ տեղեկությունները:



Ինչպես տեսնում եք, անձնական կյանքի տվյալներն այնպիսի տեղեկություններ են, որոնք կապված են մարդու առօրյայի, նրա կյանքի ընթացքի, նրա կյանքի հանգամանքների եւ պայմանների հետ, մարդու ընտանիքի, նրա ամուսնության հանգամանքների, կենցաղի եւ առհասարակ մարդու անհատականության հետ:

Օրինակ՝ մարդու **անձնական կյանքի վերաբերյալ** տեղեկություններ են նրա անձնական ապրումները, կարծիքները, ձեռքբերումները, նախասիրությունները, սովորությունները, բնավորությունը, համակրանքները եւ հակակրանքները եւ այլն:

Ինքնուրույն բովանդակություն ունի նաեւ **ընտանեկան կյանքի** վերաբերյալ տեղեկությունը. օրինակ՝ ընտանեկան կյանքի վերաբերյալ տեղեկություններ են երեխաների դաստիարակության մեթոդները, ընտանեկան հարաբերությունները, ամուսնության հանգամանքները եւ ընտանեկան մթնոլորտը:

Անձնական կյանքի տվյալների հասկացության մեջ նկարագրված տեղեկություններից, թերեւս, ամենաանհասկանալին **ֆիզիոլոգիական** վիճակի վերաբերյալ տեղեկությունն է: Այս տվյալները կապված են մարդու ֆիզիոլոգիական պահանջմունքների բավարարման հետ եւ վերաբերում են, օրինակ, մարդու հանգստին, զվարճանքին, ժամանցին եւ այլն:

- *Անձնական կյանքի տվյալները մարդու մասին այնպիսի տեղեկություններ են, որոնց մարդը սովորաբար չի ցանկանում հաղորդակից դարձնել ուրիշներին: Դա մարդու կյանքի այն մասն է, որն, ի տարբերություն մարդու հանրային կյանքի, անձեռնմխելի է շրջապատի համար: Բնականաբար, անձնական կյանքի տվյալների հրապարակումը կամ տարածումն այլոց, օրինակ՝ հարեւանների շրջանում, կարող է տհաճ լինել մարդու համար, առաջացնել անհարմարություն եւ անհանգստացնել նրան: Այդ է պատճառը, որ անձնական կյանքի տվյալներն այնպիսի տեղեկություններ են, որոնք հավակնում են լինել անձնական կյանքի գաղտնիք:*

- *Այս համատեքստում պետք է նշել, որ երեխան ոչնչով չի զիջում չափահասին. նա նույնպես ունի անձնական կյանք, ունի ապրումներ, երազանքներ, ցանկություններ, վաղ տարիքից աստիճանաբար զարգացնում է իր անհատականությունը եւ ունի իր անհատականության պաշտպանության իրավունք: Ավելին, անձնական տվյալներ մշակողները պետք է ձեռնպահ մնան երեխայի անձնական տվյալներն անհարկի մշակելու միջոցով նրա անձնական կյանք ներխուժելուց, իսկ երեխայի օրինական ներկայացուցիչները՝ ծնողները կամ խնամակալը, ինչպես նաեւ երեխայի համար պատասխանատու մարդիկ ու կառույցները, պետք է ավելի բծախնդիր լինեն երեխայի անձնական տվյալների պաշտպանության հարցում՝ երեխայի անհատականության ձեւավորման իրավունքը չխեղաթյուրելու համար:*

- Անձնական տվյալների հաջորդ տեսակը **կենսաչափական անձնական տվյալներն** են: Այս տվյալները նաեւ կոչվում են բիոմետրիկ:

Կենսաչափական անձնական տվյալներ են համարվում մարդու անձի ֆիզիկական, ֆիզիոլոգիական եւ կենսաբանական առանձնահատկությունները բնութագրող տեղեկությունները:

Նկատու՞մ եք՝ **ֆիզիկական** և **ֆիզիոլոգիական** բառերը հանդիպում են ե՛ւ անձնական կյանքի տվյալների հասկացության մեջ, ե՛ւ կենսաչափական անձնական տվյալների հասկացության մեջ: Սակայն, ավելի ուշադիր լինելու

դեպքում պարզ կլինի, որ անձնական կյանքի տվյալներ են մարդու ֆիզիկական եւ ֆիզիոլոգիական **վիճակի վերաբերյալ** տեղեկությունները, իսկ կենսաչափական են մարդու ֆիզիկական եւ ֆիզիոլոգիական **առանձնահատկությունները բնութագրող** տեղեկությունները:

Կենսաչափական անձնական տվյալներն ունեն իրենց առանձնահատկությունները. դրանք որպես կանոն՝

ա) շատ մոտ են մարդուն, եւ դրանք հնարավոր է ստանալ միայն մարդուց, անհրաժեշտ է մարդու ֆիզիկական ներկայությունը.

բ) թույլ են տալիս անսխալական նույնականացնել մարդուն, քանի որ ունիկալ են, վերաբերում են (պատկանում են) միայն մի մարդու եւ չեն կրկնվում:

Այսպես, կենսաչափական անձնական տվյալներ են օրինակ մատնահետքը, մարդու աչքի ցանցաթաղանթը, լուսանկարը (հավանաբար լսել եք կենսաչափական (բիոմետրիկ) լուսանկարների մասին, որոնք պահանջում են դեսպանատները՝ իրենց երկրների մուտքի վիզաներ տրամադրելու համար), ԴՆԹ կոդը, ստորագրությունը, ձայնը եւ այլն: Կենսաչափական անձնական տվյալների առանձնահատկությունները ցույց տալու ամենալավ օրինակը մատնահետքն է:

Նախ պարզենք առաջին չափանիշը՝ արդյոք հնարավո՞ր է ստանալ մարդու մատնահետքը, եթե մարդն այն որեւէ տեղ չի թողել: Բնականաբար, անհնար է, քանի որ դիտավորյալ կամ պատահաբար, սակայն անհրաժեշտ է, որ մարդն անձամբ թողնի իր մատի դրոշմը: Եթե մարդը չթողնի իր մատնահետքը, ապա այլ կերպ այլ աղբյուրից այն ստանալ հնարավոր չէ:

Այժմ անդրադառնանք երկրորդ չափանիշին. համահայտնի փաստ է, որ ամեն մատնահետք ունիկալ է, անկրկնելի: Հայտնի է, որ անգամ միաբջիջ երկվորյակների մոտ, որոնք արտաքնապես շատ նման են իրար եւ միեւնույն սեռի են լինում, մատնահետքերը տարբեր են եւ չկրկնվող:

- *Իրենց առանձնահատկությունների պատճառով կենսաչափական անձնական տվյալները համարվում են զգայուն անձնական տվյալներ, քանի որ դրանք մարդուն անսխալական նույնականացնելու հնարավորություն են տալիս: Ուստի, այս տվյալներն առանձնահատուկ պաշտպանության կարիք ունեն, եւ չպետք է օգտագործվեն, եթե առանց դրանց՝ այլ տվյալների միջոցով, հնարավոր է հասնել անձնական տվյալների մշակման նպատակին:*

- *Հաշվի առնելով, որ երեխան չի կարող ինքնուրույն լիարժեք պաշտպանել իր անձնական տվյալները եւ ամբողջությամբ գիտակցված որոշմամբ թույլատրել կամ արգելել իր կենսաչափական տվյալների օգտագործումը՝ պետք է նշել, որ երեխայի կենսաչափական տվյալներին պետք է առանձնահատուկ ուշադրություն դարձնել: Երեխայի կենսաչափական տվյալները կարելի է օգտագործել, այդ թվում՝ հրապարակել միայն բացառիկ դեպքերում, եթե այլ կերպ հնարավոր չէ հասնել սահմանված նպատակին, ինչպես նաեւ, երբ կենսաչափական տվյալների մշակումն անհրաժեշտ է երեխայի լավագույն շահի պաշտպանության համար (երեխայի լավագույն շահի մասին կխոսենք հաջորդիվ՝ ուղեցույցի 3-րդ բաժնում):*

- Անձնական տվյալների եւս մի տեսակ կա, որը կենսաչափականի հետ մեկտեղ համարվում է զգայուն: Դրանք **հատուկ կատեգորիայի անձնական տվյալներն** են:

Հատուկ կատեգորիայի անձնական տվյալները սպառիչ ցանկ ունեն: Այսպես, հատուկ կատեգորիայի են համարվում մարդու

- ռասայական,
- ազգային պատկանելությանը կամ էթնիկ ծագմանը,
- քաղաքական հայացքներին,
- կրոնական կամ փիլիսոփայական համոզմունքներին,
- արհեստակցական միությանն անդամակցությանը,
- առողջական վիճակին,
- սեռական կյանքին վերաբերող տեղեկությունները:

Ուշադիր նայեք այս ցանկին. երբեւէ չե՞ք հանդիպել նման ձեւակերպման: Հիշեցնենք. «Խտրականությունը, կախված սեռից, ռասայից, մաշկի գույնից, էթնիկ կամ սոցիալական ծագումից, գենետիկական հատկանիշներից, լեզվից, կրոնից, աշխարհայացքից, քաղաքական կամ այլ հայացքներից (...) արգելվում է»: Ըստ էության, հատուկ կատեգորիայի անձնական տվյալների ցանկը վկայում է, որ այն խտրականության արգելքի վերաբերյալ է: Այդ պատճառով է, որ հատուկ կատեգորիայի անձնական տվյալները նույնպես համարվում են զգայուն տվյալներ:

- *Եթե որեւէ մեկը ցանկանում է մշակել հատուկ կատեգորիայի անձնական տվյալներ, ապա բավականին ամուր հիմք եւ օրինական ու հիմնավոր*

նպատակ պետք է ունենա: Հակառակ դեպքում կարող է կասկած առաջանալ, որ տվյալներն օգտագործվում են կամ կարող են օգտագործվել խտրական վերաբերմունք դրսեւորելու համար:

- *Հաշվի առնելով երեխայի առանձնահատկությունները եւ լրացուցիչ պաշտպանություն անհրաժեշտությունը՝ չպետք է մշակվեն երեխայի այնպիսի տվյալներ, որոնք կարող են խտրականությունների պատճառ լինել: Ամենից հաճախ երեխաների նկատմամբ խտրականությունների առիթ կարող են դառնալ հենց հատուկ կատեգորիայի անձնական տվյալները: Այդ պատճառով էլ երեխայի հատուկ կատեգորիայի անձնական տվյալները կենսաչափական տվյալների նմանությամբ պետք է մշակվեն միայն խիստ անհրաժեշտ դեպքերում, երբ առկա է նման տվյալները մշակելու օրինական հիմնավոր նպատակ, եւ հատուկ կատեգորիայի տվյալների մշակումն անհրաժեշտ է երեխայի լավագույն շահի պաշտպանության համար:*

- Անձնական կյանքի տվյալները, կենսաչափական անձնական տվյալներն ու հատուկ կատեգորիայի անձնական տվյալներն առանձնացված են, որովհետեւ ունեն առանձնահատկություններ, ունեն զգայունություն եւ առանձնահատուկ ուշադրության կարիք: Սակայն մարդու վերաբերյալ այն տեղեկությունները, որոնք չեն մտնում նշված տեսակներից որեւէ մեկի մեջ, միեւնույն է, **շարունակում են լինել անձնական տվյալներ,** եւ դրանք նույնպես պաշտպանելու կարիք կա:

Անձնական տվյալների հաջորդ տեսակը, որը ցանկանում ենք ներկայացնել, փոքր ինչ տարօրինակ հատկություն ունի. այն իրականում ոչ թե անձնական տվյալի տեսակ է, այլ անձնական տվյալների կարգավիճակ է (կամ ռեժիմ): Այդ տվյալները կոչվում են **հանրամատչելի անձնական տվյալներ.** դրանց հասկացությունը հետեւյալն է՝ տեղեկություններ, որոնք տվյալների սուբյեկտի համաձայնությամբ կամ իր անձնական տվյալները հանրամատչելի դարձնելուն ուղղված գիտակցված գործողությունների կատարմամբ մատչելի են դառնում որոշակի կամ անորոշ շրջանակի անձանց համար, ինչպես նաև այն տեղեկությունները, որոնք օրենքով նախատեսված են որպես հանրամատչելի տեղեկություններ.

- *Հիշու՞մ եք՝ տվյալների սուբյեկտն այն մարդն է, ում վերաբերում են անձնական տվյալները:*

Եւ այսպես, հանրամատչելի են այն անձնական տվյալները, որոնք կամ մարդն ինքն է իր կամքով ինքնուրույն հասանելի դարձրել այլոց համար, կամ իր համաձայնությամբ են դրանք դարձել ուրիշներին հասանելի: Առանց մարդու

ցանկության՝ իր անձնական տվյալները կարող են հանրամատչելի դառնալ միայն եթե այդպես սահմանվի որեւէ օրենքով:

Օրինակ, ժամանակին կային հեռախոսային տեղեկատուներ՝ հաստափոր գրքեր էին, որոնցում ըստ ազգանունների նշված էին քաղաքի բնակիչները՝ քաղաքային հեռախոսահամարների բաժանորդները, եւ կարելի էր այդ գրքով գտնել ծանոթին կամ բարեկամին կամ ընկերոջը, տեսնել հեռախոսահամարը եւ զանգել: Մեր օրերում նման գրքերը փոխարինվել են առցանց տեղեկատուներով, որտեղ մարդկանց համաձայնությամբ ներառվում են նրանց հեռախոսահամարները, նաեւ հասցեները եւ այլ անձնական տեղեկություններ: Նմանատիպ գրքային կամ առցանց տեղեկատուներում ներառված անձնական տվյալները հասանելի են ցանկացածին, ուստի դրանք հանրամատչելի անձնական տվյալներ են:

Պետք է նշել, որ հաշվի առնելով երեխաներին պաշտպանելու անհրաժեշտությունը, որպես կանոն օրենքներով չեն սահմանվում այնպիսի հանրամատչելի աղբյուրներ, որտեղ բոլորի համար հասանելի ձեւով ներկայացված կլինեն երեխաներին նույնականացնող տվյալներ: Հետեւաբար, երեխաների անձնական տվյալները սովորաբար հանրամատչելի են դարձնում կամ նրանց տվյալները մշակողները, կամ էլ նրանց ծնողները, խնամակալները, կամ երեխայի համար պատասխանատու մարդիկ ու կառույցները: Հաճախ էլ, առանց գիտակցելու, իրենց տվյալները հանրամատչելի են դարձնում հենց երեխաները:

Ստացվում է, որ ե՛ւ անձնական կյանքի տվյալները, ե՛ւ կենսաչափական անձնական տվյալները, ե՛ւ հատուկ կատեգորիայի անձնական տվյալները ե՛ւ այլ անձնական տվյալներ կարող են դառնալ հանրամատչելի: Օրինակ, եթե ծնողն իր երեխայի առողջական վիճակի մասին տեղեկությունը, ասենք՝ ախտորոշումը, տեղադրի սոցիալական ցանցի բաց խմբում՝ այլ օգտատեր ծնողներից երեխայի հիվանդության վերաբերյալ խորհուրդ ստանալու համար, կստացվի, որ ծնողը հանրամատչելի է դարձրել երեխայի հատուկ կատեգորիայի անձնական տվյալը: Կամ եթե երեխայի դպրոցը կամ մանկապարտեզը երեխայի եւ նրա ընտանիքի սոցիալական վիճակի վերաբերյալ տեղեկություններ հայտնեն լրատվամիջոցներին, ապա հանրամատչելի կդարձնեն երեխայի անձնական կյանքի տվյալները: Մեկ այլ օրինակ՝ եթե համացանցին հասանելիություն ունեցող երեխան բոլորի համար բաց որեւէ հարթակում տեղադրի իր կենցաղի մասին պատմող լուսանկարները, իր մտքերը, իր ապրումները, տեղեկություններ իր

զգացմունքների մասին, ապա կստացվի, որ հանրամատչելի է դարձրել իր անձնական կյանքի տվյալները:

Երեխաները դեռահաս տարիքում կարող են չգիտակցված, չկշռադատված հրապարակումներ կատարել համացանցում, և արդեն չափահաս դառնալուց հետո դրանք կարող են վնասել նրանց հեղինակությանը: Իրականում, հաճախ ծնողներն են չգիտակցելով հրապարակում երեխաների վերաբերյալ այնպիսի տեղեկություններ, որոնք թեեւ առաջին հայացքից կարող են անվնաս թվալ, սակայն դեռեւս համացանցում մնացած լինելով կարող են տարիներ հետո երեխայի չափահաս դառնալուց հետո անգամ վնասել նրան (օրինակ, վերեւում մեր ներկայացրած օրինակի դեպքում, երբ ծնողը հանրամատչելի է դարձնում իր երեխայի առողջական վիճակի վերաբերյալ տվյալը):

- *Պետք է նկատի ունենալ, որ համացանցում հրապարակային դրված անձնական տեղեկության տարածումն այլեւս փաստացի վերահսկել հնարավոր չէ: Համացանցում, մասնավորապես՝ սոցիալական ցանցերում, մարդիկ իրենց մասին բազմաթիվ տեղեկություններ են տեղադրում: Սակայն, նման քանակի անձնական տվյալների տարածումը կարող է հատկապես բացասական ազդեցություն ունենալ երեխաների համար: Օրինակ, համացանցում երեխա ժամանակ կատարած հրապարակումները կարող են շատ տարիներ անց հեշտությամբ հասանելի լինել գործատուին, արդեն մեծ տարիքում ձեռք բերած ընկերներին եւ ծանոթներին, ինչու ոչ՝ նրա երեխաներին եւ սկսեն անհանգստացնել մարդուն, միջամտել նրա կյանքին եւ ստիպել վատ զգալ: Անգամ հնարավոր է, որ երեխա ժամանակ հրապարակված անձնական զգայուն տեղեկությունը հետագայում խտրական վերաբերմունքի, ասենք՝ աշխատանքի ընդունելը մերժելու առիթ դառնա:*

Համացանցում անձնական տվյալների պաշտպանության լավագույն եղանակը զգուշավորություն ցուցաբերելն է. ծնողները, երեխայի անձնական տվյալներ մշակողները պետք է միշտ ծանրութեթեւ անեն՝ արդյո՞ք հրապարակված տվյալներով չեն վնասի երեխային տարիներ հետո: Նմանապես երեխաները, որոնք

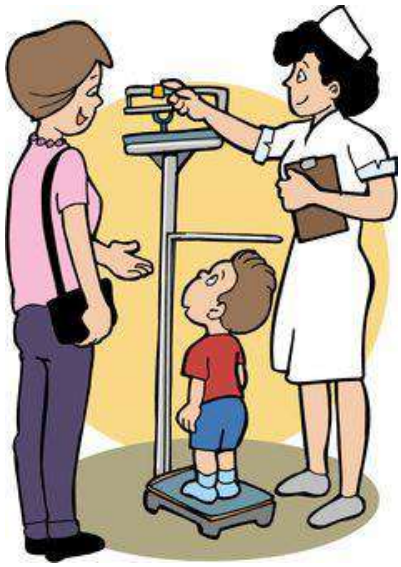
բավական մեծ են սոցիալական ցանցերից օգտվելու համար (այդ մասին կխոսենք ուղեցույցի 3-րդ բաժնում) իրենք էլ պետք է գնահատեն՝ արդյո՞ք իրենց մասին այս կամ այն տվյալը հրապարակելիս չեն վնասի իրենց տարիներ անց:

Անձնական տվյալների մշակման սկզբունքները

Երեխաների անձնական տվյալների պաշտպանությունն իրականացվում է անձնական տվյալների պաշտպանությանը բնորոշ մի քանի սկզբունքների եւ երեխաների պաշտպանությանը բնորոշ մի սկզբունքի համակցության հիման վրա:

- Անձնական տվյալների պաշտպանության իրականացման սկզբունքներից մեկն **օրինականության սկզբունքն** է: Այս սկզբունքը պահանջում է, որ անձնական տվյալները մշակվեն բացառապես օրինական եւ որոշակի նպատակներով, ինչպես նաեւ առկա լինի տվյալների մշակման հիմք:

Ի՞նչ է սա նշանակում: Օրինական եւ որոշակի նպատակ ունենալու պահանջը նշանակում է, որ երեխայի անձնական տվյալները չեն կարող օգտագործվել, ասենք՝ հրապարակվել **հենց այնպես, աննպատակ:** Պարտադիր պետք է առկա լինի **օրինական** (այսինքն՝ ոչ հանցավոր, ոչ չարամիտ, օրենքներին համապատասխանող) եւ **որոշակի** (այսինքն՝ հստակ ձեւակերպված, հասկանալի, ոչ անորոշ) նպատակ: Օրինակ, երեխային դպրոց ընդունելը եւ նրա կրթությունն ապահովելը հստակ եւ օրինական նպատակ է, որի շրջանակներում դպրոցը ստանում եւ մշակում է երեխայի որոշակի անձնական տվյալներ (անուն, ազգանուն, տարիք, հասցե եւ այլն):



Սակայն միայն օրինական եւ որոշակի նպատակի առկայությունը բավական չէ, որ տվյալների մշակումը համարվի օրինական: Անհրաժեշտ է նաեւ, որ նպատակի հետ մեկտեղ միաժամանակ առկա լինի նաեւ տվյալները մշակելու հիմք: Անձնական տվյալներ մշակելու հիմքերը 3-ն են՝

- տվյալների սուբյեկտի համաձայնությունը,
- օրենքով նախատեսված լինելը,
- տվյալը հանրամատչելի աղբյուրից ձեռք բերված լինելը:

Օրենքով նախատեսված լինելու հիմքը հազվադեպ է խնդիրներ առաջացնում, որովհետեւ օրենքներով, որպես կանոն, նկարագրված են լինում տվյալներ մշակելու պայմանները, տվյալներն օգտագործելու կարգը, տվյալներ մշակողի պարտականությունները եւ տվյալների սուբյեկտի իրավունքները:

- *Եթե չեք հիշում, ով է համարվում տվյալների սուբյեկտ եւ ով է տվյալներ մշակողը, ապա վերընթերցեք ուղեցույցի 1-ին բաժինը:*

Ինչպես նշվեց, անձնական տվյալների մշակումն օրինական է համարվում նաեւ այն դեպքում, երբ օգտագործվում են **հանրամատչելի աղբյուրից ձեռք բերված տվյալներ:** Ճիշտ է՝ անձնական տվյալները կարող են հանրամատչելի դառնալ կամ օրենքներով նախատեսված լինելու դեպքում, կամ էլ մարդու համաձայնությամբ, սակայն հաշվի առնելով այն հանգամանքը, որ ե՛ւ երեխաներն են հրապարակում իրենց վերաբերյալ տեղեկություններ, ե՛ւ մեծերն են հրապարակում իրենց երեխաների վերաբերյալ տեղեկություններ՝ եւս մեկ անգամ հարկ է նշել. պետք չէ անհարկի հրապարակել եւ հանրամատչելի դարձնել երեխաների վերաբերյալ տեղեկությունները, հատկապես՝ զգայուն անձնական տվյալները, քանի որ հնարավորություն եք տալիս ուրիշներին օգտվել այն հանգամանքից, որ տվյալները հանրամատչելի են դարձել եւ օգտագործել դրանք, տարածել եւ հետագայում նաեւ միջամտել երեխայի անձնական կյանքին:

Ամեն դեպքում, անձնական տվյալների մշակման հիմնական իրավական հիմքը տվյալների սուբյեկտի **համաձայնությունն** է: Այսպես, համաձայնություն է ցանկացած կամահայտնություն, որով տվյալների սուբյեկտը տալիս է իր հավանությունը եւ այն պետք է լինի ազատ տրված, որոշակի եւ տեղեկացված: Ինչպես տեսնում եք համաձայնությունն ունի բովանդակություն, ունի չափանիշներ եւ ցանկացած «այո», անկախ նրանից, թե որքան բարձր ասված կլինի կամ գլխի շարժումը, անկախ նրանից, թե որքան հստակ կլինի, դեռեւս չի նշանակում, որ առկա է անձնական տվյալներ մշակելու համաձայնություն: Միաժամանակ 4 չափանիշ պետք է առկա լինի, որ տվյալներ մշակելու համաձայնությունը համարվի տրված:

- *<u>Չափանիշ 1</u> - **«ցանկացած կամահայտնություն, որով տվյալների սուբյեկտը տալիս է իր հավանությունը»** - սկզբունքորեն չկան սահմանափակումներ, թե համաձայնությունն ինչ ձեւով պետք է վերցվի, սակայն այն պետք է լինի **կամահայտնություն:** Համաձայնությունը կարող է տրվել գրավոր, կամ բանավոր, կամ գործողության միջոցով, որն ակնհայտ վկայում է համաձայնության մասին: Թեեւ համաձայնությունը կարող է տրվել ցանկացած ձեւով, սակայն այն պետք է հստակ արտացոլի տվյալների սուբյեկտի կամքն 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, իսկ եթե կա տվյալների սուբյեկտի մտադրության վերաբերյալ ողջամիտ կասկած, ապա համաձայնությունը չի կարող համարվել միանշանակորեն տրված:*

- *<u>Չափանիշ 2</u> - **«ազատ տրված»** - համաձայնությունը կարող է վավեր համարվել, եթե տվյալների սուբյեկտը համաձայնությունը տվել է իր իրական ընտրությամբ (ազատ, կամավոր որոշմամբ), առանց խաբեության, սպառնալիքի, հարկադրանքի կամ համաձայնություն չտալու դեպքում իր համար բացասական հետեւանքի: Եթե համաձայնություն տալ կամ չտալու հետեւանքները խաթարում են անձի ազատ ընտրությունը, ապա համաձայնությունը չի համարվի ազատ տրված:*

- *<u>Չափանիշ 3</u> - **«որոշակի»** - համաձայնությունը կարող է վավեր համարվել, եթե այն **կոնկրետ է:** Այլ կերպ ասած, ընդհանուր համաձայնությունը, առանց անձնական տվյալի ճշգրիտ նպատակը մանրամասնելու, ընդունելի չէ: Համաձայնությունը պետք է լինի հասկանալի, այսինքն, այն պետք է վերաբերի անձնական տվյալների մշակման հստակ եւ ճշգրիտ շրջանակի:*

- *<u>Չափանիշ 4</u> - **«տեղեկացված»** - անձնական տվյալների սուբյեկտի համաձայնությունը պետք է հիմնված լինի անձնական տվյալների մշակման հանգամանքները եւ հետեւանքները գիտակցելու եւ հասկանալու, անձնական տվյալների մշակման (մշակվող տվյալների, մշակման նպատակի, այլ 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»:*

Հստակեցնենք՝ եթե անձնական տվյալների մշակումը նախատեսված չէ օրենքով, ապա այն օրինական է, եթե առկա է անձնական տվյալների մշակման վերաբերյալ տվյալների սուբյեկտի համաձայնությունը:

Ուղեցույցի 1-ին բաժնում արդեն նշել ենք, որ երեխայի անձնական տվյալների սուբյեկտը հենց երեխան է: Միաժամանակ, վերեւում էլ նշեցինք, որ անձնական տվյալների մշակման համաձայնությունը տալիս է տվյալների սուբյեկտը: Այստեղ առաջ են գալիս մի քանի հարցեր. արդյո՞ք երկու, երեք կամ չորս տարեկան երեխայից պետք է ստանալ համաձայնություն ասենք նրա նկարը սոցիալական ցանցում տեղադրելու համար: Արդյո՞ք ծնողը նույնպես պետք է ստանա երեխայի համաձայնությունը, երբ նույնպես ուզում է նրա նկարը տեղադրել սոցիալական ցանցի իր էջում: Քանի՞ տարեկանից է երեխան ինքնուրույն որոշումներ կայացնում իր տվյալների օգտագործման վերաբերյալ եւ այլն:

Թեեւ երեխա է համարվում մինչեւ 18 տարեկան մարդը, սակայն 16 տարեկանից սկսած երեխան ինքնուրույն է որոշում իր անձնական տվյալների ճակատագիրը եւ ինքն էլ տալիս է իր տվյալներն օգտագործելու համաձայնությունը կամ հակառակը՝ արգելում է դրանք օգտագործել: Իսկ մինչեւ 16 տարեկան երեխայի անձնական տվյալները մշակելու համար համաձայնությունը տալիս է նրա օրինական ներկայացուցիչը՝ ծնողը, խնամակալը, հոգաբարձուն կամ որդեգրողը:

- *Երեխայի կարծիքը երեխայի զարգացվածության աստիճանին զուգընթաց պետք հաշվի առնվի նրան վերաբերող հարցերում: Թեեւ ծնողներն են կայացնում 16 տարեկանից փոքր երեխայի անձնական տվյալների հետ կապված որոշումներ, սակայն եթե երեխան բավական զարգացած եւ գիտակից է, որ դիրքորոշում հայտնի իր տվյալների օգտագործման վերաբերյալ, ապա ծնողները պետք է խորհրդակցեն նրա հետ եւ հաշվի առնեն նրա կարծիքը:*

Ընդունված է, որ 13 տարեկան երեխան արդեն ունի բավարար իրավագիտակցություն, որպեսզի մասնակցի իր անձնական տվյալների մշակման վերաբերյալ որոշումների կայացմանը եւ մեծերն այդ տարիքի երեխայի կարծիքն արդեն պետք է պարտադիր հաշվի առնեն: Պատահական չէ, որ, որպես կանոն, սոցիալական ցանցերը հենց 13 տարեկանից սկսած են երեխաներին իրավունք տալիս ունենալ ինքնուրույն հաշիվներ (էջեր):

- *Հաշվի առնելով, որ տեղեկատվության առատության այս դարում երեխաներն ավելի արագ են զարգանում, ավելի շուտ են ձեռք բերում իրավագիտակցություն, ինչպես նաեւ հաշվի առնելով, որ ամեն երեխա անհատականություն է՝ Անձնական տվյալների պաշտպանության գործակալությունն, օրինակ, հաշվի է առնում 13 տարեկանից ցածր տարիքի երեխաների կարծիքն իրենց տվյալների օգտագործման վերաբերյալ:*

Եվս մի կարեւոր նկատառում ծնողների (այլ օրինական ներկայացուցիչների) համար. պետք է նկատի ունենալ, որ մինչեւ 16 տարեկան երեխայի անձնական տվյալների վերաբերյալ որոշումներ կայացնելիս ծնողները կամ այլ օրինական ներկայացուցիչները հանդես են գալիս երեխայի, այլ ոչ թե իրենց անունից: Սա նշանակում է, որ ծնողը կամ այլ օրինական ներկայացուցիչները չպետք է երեխայի անձնական տվյալների մշակումը հարմարեցնեն իրենց շահին, իսկ եթե պարզվի, որ երեխայի անձնական տվյալների մշակման հարցում ծնողի շահը հակասության

մեջ է մտնում երեխայի շահի հետ, ապա առավելությունը պետք է տրվի երեխայի շահին: Օրինակ, եթե դպրոցն առաջարկում է ծնողին համաձայնություն տալ, որ երեխային դպրոցում գտնվելու ամբողջ ընթացքում տեսանկարահանեն եւ առցանց հեռարձակեն, եւ ծնողը կարողանա հետեւել երեխային, ապա ծնողը կանգնում է երկընտրանքի առաջ. մի կողմից խոսքն այն մասին է, որ երեխային առցանց հետեւելով ծնողը հանգիստ կլինի, որ երեխայի հետ ամեն ինչ կարգին է (ծնողի շահ), մյուս կողմից էլ՝ երեխայի՝ իր անհատականությունն աստիճանաբար զարգացնելու իրավունքը կխեղաթյուրվի, եթե վաղ հասակից սկսած երեխան բնականոն երևույթ համարի իրեն տեսահսկելը (երեխայի շահ): Այս դեպքում ծնողը պետք է հրաժարվի երեխայի տվյալները մշակելու համաձայնություն տալուց՝ հաշվի առնելով ոչ թե իր, այլ երեխայի շահը:

- Քանի որ խոսեցինք երեխայի շահից, ապա անդրադառնանք երեխաների պաշտպանությանը բնորոշ ամենակարեւոր սկզբունքներից մեկին՝ **երեխայի լավագույն շահի սկզբունքին:** Երեխայի լավագույն շահի սկզբունքի էությունն է ապահովել երեխայի ֆիզիկական, հոգեբանական և բարոյական առողջ զարգացումը, այլ կերպ ասած՝ նպաստել երեխայի անհատականության բնականոն զարգացմանը:

Երեխայի անձնական տվյալների պաշտպանությունն ինքնին բխում է երեխայի լավագույն շահի սկզբունքից, սակայն, երբեմն երեխայի լավագույն շահը և նրա անձնական տվյալների պաշտպանությունը կարող են միմյանց հակադրվել: Այս դեպքում նախապատվությունը տրվում է երեխայի լավագույն շահին: Օրինակ, եթե վտանգի տակ է երեխայի կյանքը կամ առողջությունը, եւ երեխային փրկելու համար անհրաժեշտ է «զոհել» երեխայի անձնական տվյալները (հրապարակել կամ այլ կերպ մշակել), ապա այս դեպքում նախապատվությունը տրվում է երեխայի լավագույն շահին, այն է՝ կյանքը փրկելուն:

- Անձնական տվյալների պաշտպանության բավականին պարզ, սակայն անչափ կարեւոր սկզբունքներից է **համաչափության սկզբունքը:**

Համաչափության սկզբունքը պահանջում է, որ անձնական տվյալները մշակվեն այն **նվազագույն քանակով** եւ պահպանվեն այն **նվազագույն ժամկետով,** որն անհրաժեշտ է օրինական նպատակներին հասնելու համար: Այս սկզբունքի համաձայն՝ արգելվում է այնպիսի անձնական տվյալների մշակումը, որոնք անհրաժեշտ չեն տվյալները մշակելու նպատակի համար, իսկ տվյալները մշակելու նպատակին հասնելու միջոցները պետք է լինեն պիտանի, անհրաժեշտ և չափավոր:

Օրինակ, պատկերացրեք՝ դպրոցի միջանցքում տեղադրված է տեսախցիկ, որի նպատակն է տեսագրել միջանցքը դասամիջոցի ժամին կարգուկանոնը խախտողներին ճանաչելու նպատակով: Այժմ, եթե դպրոցի տնօրենը դիտել է նախորդ օրվա տեսագրությունները եւ պարզել է, որ որեւէ մեկը կարգուկանոնը չի խախտել, ապա տեսագրությունները հավելյալ ժամանակով պահելը կհակասի համաչափության սկզբունքին: Կամ, եթե դպրոցի դասասենյակում տեղադրված տեսախցիկի միակ նպատակը բացառապես դասասենյակի չհրկիզվող պահարանը հսկելն է, որ տեսախցիկը պետք է միայն պահարանը եւ դրա անմիջական շրջակայքը տեսագրի, իսկ ամբողջ դասասենյակի եւ աշակերտների տեսագրումը կհակասի համաչափության սկզբունքին:

- Վերջում անհրաժեշտ է խոսել անձնական տվյալների անվտանգության ապահովման կարեւորության մասին: Բանն այն է, որ եթե օրինական հիմքերով, օրինական նպատակով եւ համաչափության սկզբունքի պահպանմամբ մշակվեն երեխայի անձնական տվյալները, սակայն դրանք չունենան բավարար պաշտպանվածություն, միեւնույն է անձնական տվյալների պաշպանության իրավունքը կխախտվի:

Երեխաների անձնական տվյալների հետ առնչվողները, տվյալներ մշակողները պետք է **տեխնիկական եւ կազմակերպչական** միջոցառումներ ձեռնարկեն՝ երեխայի տվյալների անվտանգությունը ինչպես պատահական, այնպես էլ դիտավորյալ միջամտությունից պաշտպանելու համար:

Տեխնիկական միջոցառումները վերաբերում են այնպիսի տեխնոլոգիաների եւ տեխնիկական միջոցների կիրառմանը, որոնք կապահովեն անձնական տվյալներն անօրինական օգտագործումից, ձայնագրումից, ոչնչացումից, վերափոխումից, ուղեփակումից, կրկնօրինակումից, տարածումից և այլ միջամտությունից: Նման միջոցներ են, օրինակ, հակահրդեհային համակարգերի կիրառումը, համակարգչային հակավիրուսային ծրագրերի տեղադրումը եւ այլն:

Կազմակերպչական միջոցառումները վերաբերում են այնպիսի ընթացակարգերի եւ կանոնակարգերի կիրառմանը, որոնք կրկին կապահովեն անձնական տվյալների անվտանգությունը: Օրինակ, նման միջոցառումներ են տվյալներ մշակողի անձնակազմի վերապատրաստումը (ուսուցումը) կամ տեսահսկման ընթացակարգի ընդունումը, համակարգիչները մուտքանուններով եւ գաղտնաբառերով ապահովելու եւ դրանք թարմացնելու կարգերը, անձնական տվյալներին հասանելիություն ունեցող անձանց իրավասությունները եւ պարտականությունները սահմանելը եւ այլն:

- Ձեռնարկվող անվտանգության միջոցառումները պետք է համարժեք լինեն տվյալների տեսակին. որքան զգայուն է տվյալը, այնքան բարձր պետք է լինի ձեռնարկվող անվտանգության միջոցառումը: Այսպես, առանձնահատուկ անվտանգության միջոցառումներ պետք է ձեռնարկվեն երեխաների հատուկ կատեգորիայի եւ կենսաչափական տվյալների պաշտպանության համար:

- Ձեռնարկվող անվտանգության միջոցառումները պետք է համարժեք լինեն նաեւ տվյալների անվտանգությանը սպառնացող ռիսկերին. որքան բարձր է տվյալների անվտանգությանը սպառնացող ռիսկը, այնքան բարձր պետք է լինի ձեռնարկվող անվտանգության միջոցառումը:

Թեստ 1 Անձնական տվյալների պաշտպանությունը

1. Նշվածներից որո՞նք են անձնական տվյալներ

- Անուն-ազգանուն-հայրանուն,
- Արյան խումբ, մատնահետք,
- Տեղեկություններ կրթության մասին, լուսանկարներ
- Թվարկված բոլոր տարբերակները:

2. Կարո՞ղ եք վերահսկել Ձեր լուսանկարների տարածումը համացանցում, եթե դրանք հրապարակել եք սոցիալական ցանցերում

- Այո
- Ոչ

3. Ձեր ընկերը հավաքույթ է կազմակերպել ու հրավիրել Ձեր բոլոր ընկերներին: Ճի՞շտ է արդյոք հանդիպման վայրի, օրվա ու ժամի մասին տեղեկությունը հրապարակել համացանցում՝ (սոցիալական ցանցում) բոլորի համար հասանելի ձեւով:

- Այո
- Ոչ

4. Նշվածներից որո՞նք կհրապարակեք համացանցում

- Ամեն ինչ, ինչ ծիծաղելի է ու հետաքրքիր եւ ընկերներիս դուր կգա
- Սկզբում կմտածեմ. արդյո՞ք անհարմար չեմ զգա, եթե ուրիշները տեսնեն այն, ինչ հրապարակում եմ
- Լուսանկարներ, անուն-ազգանուն-հայրանուն, հասցե

5. Կարո՞ղ է Ձեր ընկերը մտնել սոցիալական ցանցի Ձեր էջ ու Ձեր անունից հաղորդագրություններ ուղարկել

- Այո, որովհետեւ իմ ընկերն է ու ես նրան վստահում եմ
- Ոչ: Ունենալով հասանելիություն իմ էջին՝ ընկերս կարող է հասանելիություն ունենալ ոչ միայն այն տվյալներին, որ թույլ եմ տվել նայել, այլ նաև մյուս բոլոր տվյալներին

6. Ի՞նչ հետևանքներ կարող է ունենալ այն, որ Ձեր ընկերոջ լուսանկարը տարածեք համացանցում՝ նկարի վրա նշելով նրան

- Լուսանկարի զանգվածային տարածում համացանցում, եթե գաղտնիության կարգավորումները ճիշտ չեն արված
- Ոչ մի հետեւանք չի ունենա
- Ընկերս ավելի հանրահայտ կդառնա

7. Եթե խնդրում են Ձեր համաձայնությունը Ձեր անձնական տվյալներն օգտագործելու համար, ապա պարտավո՞ր են արդյոք տեղեկացնել, թե կոնկրետ ինչ տվյալներ են անհրաժեշտ, ինչ նպատակով են ցանկանում ստանա Ձեր տվյալները, ինչպես եւ ինչ պայմաններով են դրանք օգտագործելու

- Այո, ես պետք է մինչեւ համաձայնություն տալս մանրամասն եւ սպառիչ իմանամ իմ անձնական տվյալների օգտագործման բոլոր պայմանները
- Ոչ, պարտավոր չեն. չէ՞ որ հարցնում են իմ համաձայնությունը, եւ եթե ես համաձայն եմ, որ իմ տվյալներն օգտագործեն, ապա կարող են եւ չտեղեկացնել
- Պարտավոր են միայն այն դեպքում, եթե ես պահանջեմ

8. Եթե որեւէ հավելվածից օգտվելու համար Ձեզանից պահանջում են անձնական տեղեկություններ, կամ եթե անձնական տեղեկություններ է ուզում սոցիալական ցանցում Ձեր ընկերը, ում իրական կյանքում չեք ճանաչում եւ ունեք կասկածներ, ի՞նչ կանեք

- Խորհուրդ կհարցնեք
- Կտրամադրեք անձնական տվյալներն ու կսպասեք, թե ինչ է լինելու
- Չեք տրամադրի անձնական տվյալներ

**Կարող եք ընտրել ճիշտ պատասխանի մի քանի տարբերակներ*

9. Եթե անձնական տեղեկություններ է պահանջում ուսումնական հաստատությունը, օրինակ՝ դպրոցը, եւ ունեք կասկածներ կամ Ձեզ համար հստակ չէ անձնական տվյալներ պահանջելու նպատակը, ի՞նչ կանեք

- Խորհուրդ կհարցնեք
- Կտրամադրեք անձնական տվյալներն ու կսպասեք, թե ինչ է լինելու. չէ՞ որ այս անգամ պահանջողը դպրոցն է, այլ ոչ անծանոթ հավելված կամ օգտատեր
- Կհարցնեք անձնական տվյալներ պահանջելու նպատակը, ապա կորոշեք՝ տալ տվյալները միանգամից, թե ոչ
- Կհարցնեք անձնական տվյալներ պահանջելու նպատակը, սակայն չեք տրամադրի անձնական տվյալներ

**Կարող եք ընտրել ճիշտ պատասխանի մի քանի տարբերակներ*

10. Ի՞նչ կանեք, եթե Ձեր անձնական տվյալների պաշտպանության իրավունքը խախտվի կամ ունենաք նման կասկած

- Կդիմեմ ծնողներիս, մեծերին
- Կդիմեմ Անձնական տվյալների պաշտպանության գործակալությանը
- Կփորձեմ ինքնուրույն վերականգնել իմ իրավունքները. չէ՞ որ իմ անձնական տվյալների պաշտպանության իրավունքն է խախտվել

- Ոչինչ չեմ անի, միեւնույն է, այսօր գրեթե բոլորի անձնական տվյալները մատչելի են համացանցում

**Կարող եք ընտրել ճիշտ պատասխանի մի քանի տարբերակներ*

Թեստ 2 Պարզեք, թե որքանով են Ձեր տվյալները պաշտպանված համացանցում

1. Օգտագործու՞մ եք Ձեր ծննդյան օրվա տվյալները որպես գաղտնաբառ

1. Այո
2. Ոչ
3. Միայն այն հարթակներում, որոնցում տվյալների պաշտպանությունն ինձ համար կարևոր չէ

2. Օգտագործու՞մ եք միևնույն գաղտնաբառը բոլոր հարթակներում

1. Այո
2. Ոչ
3. Հազվադեպ

3. Որքա՞ն հաճախ եք փոխում գաղտնաբառը

1. Տարին մեկ անգամ, ոչ ավելի հաճախ
2. Ամիսը մեկ անգամ կամ ավելի հաճախ
3. Չեմ հիշում՝ վերջին անգամ երբ եմ փոխել

4. Այլ հարթակներին կցելու համար օգտագործու՞մ եք հավելյալ էլեկտրոնային հասցե

1. Ոչ, ունեմ էլեկտրոնային մեկ հասցե բոլոր նպատակների համար
2. Այո, ես օգտագործում եմ էլեկտրոնային հավելյալ հասցե
3. Ես էլեկտրոնային մի քանի հասցեներ ունեմ, նրանցից յուրաքանչյուրը կցված է տարբեր հարթակների

5. Հաճա՞խ եք օգտագործում այնպիսի ծրագրեր, որոնք պահանջում են Ձեր տվյալները. օրինակ՝ գտնվելու վայրը կամ հասցեագիրքը

1. Ոչ, երբեք
2. Եղել է մի քանի անգամ
3. Հաճախ

6. Հաճա՞խ եք օգտվում չպաշտպանված, բաց Wi-Fi-ներից

1. Երբեք

2. Երբեմն պետք է լինում
3. Նման մանրուքների ուշադրություն չեմ դարձնում

7. Օգտվու՞մ եք երկփուլանի վավերացումից. օրինակ՝ գաղտնաբառ + հաստատում SMS-ի միջոցով

1. Ոչ, դա ավելորդ է
2. Այո
3. Միայն կարեւոր գործարքներ կամ գործողություններ անելիս

Թեստ 1-ի ճիշտ պատասխանները

Հարց 1

Ճիշտ պատասխանն է 4-րդ տարբերակը՝ «Թվարկված բոլոր տարբերակները»։

- *Անձնական տվյալ են համարվում բոլոր այն տեղեկությունները, որոնցով կարելի է մարդուն նույնականացնել, այն տեղեկությունները, որոնք վերաբերում են մարդուն։*

Հարց 2

Ճիշտ պատասխանն է 2-րդ տարբերակը՝ «Ոչ»։

- *Երբ մարդու մասին տեղեկությունը հայտնվում է համացանցում, այն հասանելի է դառնում այլ մարդկանց՝ ամբողջ աշխարհով մեկ, ովքեր կարող են ներբեռնել այն, պահպանել, փոխել ու օգտագործել, ինչպես ցանկանան։ Այդ պատճառով էլ հնարավոր չէ միանշանակ վերահսկել հրապարակված լուսանկարների կամ այլ անձնական տվյալների տարածումը եւ օգտագործումը համացանցում։ Ուստի, կարևոր է չհրապարակել զգայուն տեղեկություններ ու ապահովել անձնական կյանքի գաղտնիությունը։*

Հարց 3

Ճիշտ պատասխանն է 2-րդ տարբերակը՝ «Ոչ»։

- *Անսահմանափակ թվով մարդկանց հասանելիությունը նման տվյալներին կարող է վտանգավոր կամ անհանգստացնող լինել Ձեզ ու Ձեր ընկերների համար։ Դուք չեք կարող համոզված լինել, որ այդ տեղեկությունները չեն օգտագործի Ձեր դեմ։ Օրինակ՝ Ձեր աղջիկ ընկերներից մեկի մերժված երկրպագուն կարող է այցելել ձեր հավաքույթ եւ փչացնել ինչպես ձեր աղջիկ ընկերոջ տրամադրությունը, այնպես էլ ամբողջ հավաքույթը։ Եթե ընտրել եք սոցիալական ցանցը որպես հավաքույթը կազմակերպելու ամենահարմար միջոց, ապա հանդիպման վայրի, օրվա ու ժամի վերաբերյալ տեղեկությունները հրապարակեք եւ հավաքույթի այլ կազմակերպչական հարցերը քննարկեք ոչ թե համընդհանուր հասանելի էջում կամ խմբում, այլ փակ խմբում կամ առանձին ստեղծված խմբային նամակագրությամբ, որտեղ կլինեն միայն հավաքույթին հրավիրված մարդիկ։*

Հարց 4

Ճիշտ պատասխանն է 2-րդ տարբերակը՝ «Սկզբում կմտածեմ. արդյո՞ք անհարմար չեմ զգա, եթե ուրիշները տեսնեն այն, ինչ հրապարակում եմ»

- *Ձեր մասին տեղեկությունը համացանցում օգնում է մարդկանց Ձեր մասին տպավորություններ ձեւավորել, եւ այն, ինչ հրապարակում եք Ձեր առօրյա կյանքի մասին, կարող է բացասաբար ազդել Ձեզ, Ձեր հեղինակության վրա։ Համակարգչի դիմաց նստած կամ հեռախոսով սոցիալական ցանցերում Ձեր*

մասին տեղեկություններ հրապարակային տարածելիս կամ գրառումներ անելիս երբեմն ստեղծվում է տպավորություն, որ մենակ եք Ձեր զրուցակցի, կամ ընկերների հետ: Սակայն իրականում, երբ սոցիալական ցանցերում Ձեր մասին տեղեկություն եք հրապարակում հանրամատչելի տարբերակով, լուսանկարի տարածում կամ գրառում կատարում Ձեր էջում, Ձեր տվյալները հասանելի եք դարձնում անորոշ եւ անսահմանափակ թվով անձանց՝ ուսուցիչների, ծնողների ու ընկերների, հարեւանների, ինչպես նաեւ անծանոթների համար: Պետք է նաեւ հաշվի առնել, որ այսօր հրապարակված տեղեկությունը, ըստ էության, համացանցում մնում է ընդմիշտ: Ուստի, Ձեր անձնական կյանքի մասին այսօր հրապարակված տեղեկությունները տարիներ հետո կարող են հասանելի լինել Ձեր գործատուին, ամուսնուն/կնոջը կամ երեխաներին: Այդ պատճառով պետք է լավ մտածել, թե արդյո՞ք պատրաստ եք բոլորի համար բացել Ձեր անձնական կյանքի մասին տեղեկությունները:

Հարց 5

Ճիշտ պատասխանն է 2-րդ տարբերակը՝ «Ոչ: Ունենալով հասանելիություն իմ էջին՝ ընկերս կարող է հասանելիություն ունենալ ոչ միայն այն տվյալներին, որ թույլ ես տվել նայել, այլ նաև մյուս բոլոր տվյալներին»

- *Ձեր էջը Ձեր անձնական տարածքն է, որ պարունակում է բազմաթիվ տվյալներ ոչ միայն Ձեր մասին, այլ նաև այն մարդկանց մասին, որոնց հետ շփվում եք: Թույլ տալով ընկերոջը մտնել Ձեր էջ՝ Դուք հնարավորություն եք տալիս նայել ոչ միայն մեկ հատուկ ֆայլ կամ տվյալ կամ կատարել մեկ գործողություն, այլ նաև տեսնել Ձեր էջում պահվող մյուս բոլոր տեղեկությունները: Եթե անգամ մտերիմ եք եւ դեմ չեք, որ Ձեր ընկերը տեսնի Ձեր էջում առկա ոչ հանրային (փակ, private) տեղադրված տեղեկությունները, ապա չեք կարող վստահ լինել, որ Ձեզ հետ շփվող եւ անգամ Ձեր ընկերոջը չճանաչող մարդիկ նույնպես կցանկանան, որ Ձեզ հետ իրենց խոսակցությունները, Ձեզ հետ կիսված տեղեկությունները կամ Ձեզ ուղղված անձնական հաղորդագրությունները նույնպես հասանելի դառնան Ձեր ընկերոջը. չէ՞ որ Դուք պատասխանատու եք այն տեղեկության պահպանման համար, որն այլ մարդիկ վստահել են կամ հայտնել են Ձեզ անձնական, ոչ հրապարակային նամակներով կամ գրառումներով:*

Հարց 6

Ճիշտ պատասխանն է 1-ին տարբերակը՝ «Լուսանկարի զանգվածային տարածում համացանցում, եթե գաղտնիության կարգավորումները ճիշտ չեն արված»

- *Իհարկե, Ձեր ընկերը կարող է նաեւ հայտնի դառնալ, սակայն այդ հայտնիությունը նրան կարող է ոչ թե հաճելի լինել, այլ անհանգստացնել, միջամտել նրա անձնական կյանքին: Հնարավոր է, որ Ձեր ընկերը չի*

ցանկանում, որ լուսանկարը, որում նշել եք նրան, տեսնեն այլ մարդիկ: Հիշեք, սոցիալական ցանցում հրապարակային տեղադրված լուսանկարը հասանելի է անորոշ եւ անսահմանափակ թվով անձանց, ուստի երբեք չեք կարող հստակ իմանալ, թե ով կտեսնի հրապարակային տեղադրված լուսանկարը եւ ինչպես կօգտագործի այն Ձեր ընկերոջ նկատմամբ: Հետեւաբար, այլ անձանց նկարները համացանցում հրապարակելիս, ինչպես նաեւ նրանց նշելիս հարցրեք նրանց կարծիքը եւ թույլ տվեք՝ իրենք որոշեն, թե իրենց նկարը ուզո՞ւմ են, որ հայտնվի համացանցում, թե՝ ոչ: Մի՛ տեղադրեք անձնական տեղեկություններ Ձեր ընկերների մասին առանց նրանց համաձայնության: Իսկ եթե Ձեր ընկերոջ նկարը հրապարակում եք միայն իր համար, ապա համոզվեք, որ նկարի գաղտնիության կարգավորումները ճիշտ են ընտրված, եւ նկարը ոչ թե հանրամատչելի է, այլ տեսանելի եւ հասանելի է միայն Ձեր ընկերոջ համար:

Հարց 7

Ճիշտ պատասխանն է 1-ին տարբերակը՝ «Այո, ես պետք է մինչեւ համաձայնություն տալս մանրամասն եւ սպառիչ իմանամ իմ անձնական տվյալների օգտագործման բոլոր պայմանները»

- *Ձեր անձնական տվյալներն օգտագործելու վերաբերյալ Ձեր համաձայնությունը պետք է հիմնված լինի անձնական տվյալների օգտագործման հանգամանքները եւ հետեւանքները գիտակցելու եւ հասկանալու, անհրաժեշտ անձնական տվյալների ցանկի, անձնական տվյալների օգտագործման նպատակի, անձնական տվյալների օգտագործման պայմանների եւ դրանց հետ կատարվելիք գործողությունների, այդ թվում՝ այլն անձանց հնարավոր փոխանցման վերաբերյալ ճշգրիտ եւ լիարժեք տեղեկությունների վրա: Միայն տեղեկացված համաձայնությունն է, որ կարող է համարվել վավեր: Ձեր անձնական տվյալներն օգտագործելու վերաբերյալ համաձայնություն տալուց առաջ համոզվեք, որ տեղեկացվել եք Ձեր մասին տվյալների օգտագործման բոլոր պայմանների վերաբերյալ, որպեսզի հետագայում կարողանաք պաշտպանել Ձեր տվյալները եւ Ձեր անձնական կյանքը:*

Հարց 8

Ճիշտ պատասխաններն են 1-ին եւ 3-րդ տարբերակները՝ «Խորհուրդ կհարցնեմ, չեմ տրամադրի անձնական տվյալներ»

- *Պետք չէ անծանոթ մարդկանց, անծանոթ հավելվածների անձնական տվյալներ հաղորդել: Հաճախ հավելվածները պահանջում են ավելի շատ տվյալներ, քան առաջին հայացքից անհրաժեշտ է այն օգտագործելու համար. նման դեպքերում պետք չէ ավելի շատ անձնական տվյալներ հաղորդել, բավարարվեք նվազագույնով: Եթե հավելվածն անծանոթ է կամ*

շատ տվյալներ է պահանջում եւ կասկածներ է առաջացնում, ապա խուսափեք Ձեր տվյալներին հասանելիություն տալուց: Նույնը վերաբերում է սոցիալական ցանցերի անծանոթ օգտատերերին. չեք կարող իմանալ, թե ինչպիսի մարդ է Ձեզ հետ շփվում ու ինչպես է նա օգտագործելու Ձեր տվյալները: Աշխատեք խորհրդակցել ծնողների հետ, եթե ունեք տեղեկատվական անվտանգության մասնագետ ընկերներ՝ նրանց հետ, կամ պարզապես դիմեք ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալություն՝ խորհրդատվություն ստանալու համար:

Հարց 9

Ճիշտ պատասխաններն են 1-ին եւ 4-րդ տարբերակները՝ «Խորհուրդ կհարցնեմ, կհարցնեմ անձնական տվյալներ պահանջելու նպատակը, սակայն չեմ տրամադրի անձնական տվյալներ»

- *Ճիշտ է, այս անգամ անձնական տեղեկություններ պահանջողը դպրոցն է, սակայն միշտ չէ, որ պարտավոր եք Ձեր անձնական տեղեկությունները տրամադրել անգամ դպրոցին: Բանն այն է, որ անձնական տվյալներ ուսումնական հաստատությանը կարող են անհրաժեշտ լինել տարբեր նպատակներով՝ իր բուն գործառույթներն իրականացնելու համար, կամ եթե որեւէ արտոնություն են ցանկանում առաջարկել աշակերտին (օրինակ, Ձեր ընտանիքի սոցիալական վիճակի վերաբերյալ տեղեկություն կարող են հարցնել, եթե սոցիալական վիճակով պայմանավորված՝ ցանկանում են առաջարկել դասագրքերն անվճար ստանալ կամ, օրինակ, ուսման վարձի զեղչի արտոնություն) կամ որեւէ միջոցառում կազմակերպելու համար (օրինակ, էքսկուրսիա կազմակերպելու համար ցանկանում են կոնտակտային տվյալներ) եւ այլն: Նման դեպքերում պետք չէ շտապել. եթե դպրոցը նախապես չի հիմնավորել, թե ինչու է պահանջում Ձեր մասին տեղեկություններ, ապա խնդրեք բացատրել Ձեզնից անձնական տեղեկությունները պահանջելու նպատակը, խորհրդակցեք ծնողների, մեծերի հետ, պարզեք՝ անձնական տեղեկություններ տրամադրելը Ձեր պարտականությունն է, թե դա Ձեր հայեցողությանն է թողնված, եւ եթե Ձեր հայեցողությանն է թողնված, ապա որոշեք՝ տալ տվյալներ, թե ոչ (օրինակ՝ միգուցե չեք ուզում մասնակցել էքսկուրսիային, հետեւաբար անհրաժեշտ էլ չի լինի դպրոցին տրամադրել կոնտակտային տվյալներ): Անհրաժեշտության դեպքում կարող եք նաեւ դիմել ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալություն՝ խորհրդատվություն ստանալու համար:*

Հարց 10

Ճիշտ պատասխաններն են 1-ին եւ 2-րդ տարբերակները՝ «Կդիմեմ ծնողներիս, կդիմեմ ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալությանը»

- *Եթե պարզել եք, որ Ձեր անձնական տվյալներն օգտագործվել են ոչ օրինական կերպով կամ առաջացել են նման կասկածներ, ապա միանշանակ պետք չէ ձեռքերը ծալել եւ ոչինչ չանել: Որպես առաջին քայլ հնարավորինս արագ դիմեք ծնողներին, մեծերին՝ Ձեր անձնական տվյալների նկատմամբ միջամտությունը գնահատելու եւ տվյալները պաշտպանելու հարցում խորհուրդ եւ օժանդակություն ստանալու համար: Հնարավորինս շուտ դիմեք նաեւ ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալությանը: Գործակալությունը՝որպես անձնական տվյալների պաշտպանությունն ապահովող կառույց, կարող է տրամադրել խորհրդատվություն, քննել Ձեր անձնական տվյալների օգտագործման օրինականությունը եւ խախտում հայտնաբերելու դեպքում պահանջել, որ խախտումը վերացվի, իսկ անհրաժեշտության դեպքում նաեւ դիմել իրավապահ մարմինների օգնությանը:*

Թեստ 2-ի ճիշտ պատասխանները

1-ին հարց

1-ին տարբերակ - 0 միավոր
2-րդ տարբերակ - 2 միավոր
3-րդ տարբերակ - 1 միավոր

2-րդ հարց

1-ին տարբերակ - 0 միավոր
2-րդ տարբերակ - 2 միավոր
3-րդ տարբերակ - 1 միավոր

3-րդ հարց

1-ին տարբերակ - 1 միավոր
2-րդ տարբերակ - 2 միավոր
3-րդ տարբերակ - 0 միավոր

4-րդ հարց

1-ին տարբերակ - 0 միավոր
2-րդ տարբերակ - 1 միավոր
3-րդ տարբերակ - 2 միավոր

5-րդ հարց
1-ին տարբերակ - 2 միավոր
2-րդ տարբերակ - 1 միավոր
3-րդ տարբերակ - 0 միավոր

6-րդ հարց
1-ին տարբերակ - 2 միավոր
2-րդ տարբերակ - 1 միավոր
4-րդ տարբերակ - 0 միավոր

7-րդ հարց
1-ին տարբերակ - 0 միավոր
2-րդ տարբերակ - 2 միավոր
3-րդ տարբերակ - 1 միավոր

0-5 միավոր
Ձեր տվյալները վատ են պաշտպանված։ Անհրաժեշտ է միջոցներ ձեռնարկել։ Ընտրեք բարդ գաղտնաբառեր, հաճախ փոխեք դրանք ու տարբեր հարթակներում օգտագործեք տարբեր գաղտնաբառեր։ Օգտագործեք երկփուլանի վավերացում բոլոր այն հարթակներում, որոնք ունեն այդ հնարավորությունը։

6-10 միավոր
Ձեր տվյալների պաշտպանվածությունը միջին մակարդակի է։ Տվյալների պաշտպանությանն ուղղված որոշակի միջոցառումներ իրականացնում եք, սակայն բավականաչափ բծախնդիր չեք տվյալները պաշտպանելու հարցում։ Անհրաժեշտ է մի փոքր ավելացնել տվյալների պաշտպանությունը. ընտրեք բարդ գաղտնաբառեր, հաճախ փոխեք դրանք ու տարբեր հարթակներում օգտագործեք տարբեր գաղտնաբառեր։ Օգտագործեք երկփուլանի վավերացում բոլոր այն հարթակներում, որոնք ունեն այդ հնարավորությունը։

11-14 միավոր
Ձեր տվյալները լավ են պաշտպանված։ Շարունակեք պահպանել անվտանգության նման բարձր մակարդակ։

ՀՀ արդարադատության նախարարության անձնական տվյալների
պաշտպանության գործակալություն
ՀՀ, ք. Երեւան. 0078, Հալաբյան 41
Հեռ. 010 594 192/195

Տպաքանակը՝ 300

Տպագրությունը՝ լազերային-թվային, ֆորմատ A4

«Իրավական կրթության և վերականգնողական
ծրագրերի իրականացման կենտրոն» ՊՈԱԿ

375008, ք. Երևան, Մ. Խորենացի 162ա

հեռախոս 574406, ֆաքս 574453

էլ. հասցե՝ info@lawinstitute.am

ՀՀ ԱՐԴԱՐԱԴԱՏՈՒԹՅԱՆ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

unicef