ԱԿԲԱ ԲԱՆԿԻ ԽՄԲԻ
ԳԱՂՏՆԻՈՒԹՅԱՆ ՔԱՂԱՔԱԿԱՆՈՒԹՅՈՒՆ

Հաշվառման համար	Խմբագրության համար	Հաստատման ամսաթիվ	Ուժի մեջ մտնելու ամսաթիվ
GROUP POLICY 21#6	1	01.06.2026թ.	08.06.2026թ.

Հեղինակ՝

Ստորաբաժանում	Պաշտոն	Անուն Ազգանուն
	«ԱԿԲԱ ԲԱՆԿ» ԲԲԸ Իրավաբանական և համապատասխանության տնօրեն	Զարինե Ազիզյան
	«ԱԿԲԱ ԲԱՆԿ» ԲԲԸ ՏԱ և Կիբեռանվտանգության տնօրեն	Վաղարշակ Իսկանդարյան

Նախահաստատող՝

Պաշտոն	Անուն Ազգանուն
«ԱԿԲԱ ԲԱՆԿ» ԲԲԸ Գլխավոր գործադիր տնօրեն	Հակոբ Անդրեասյան
«ԱԿԲԱ ԼԻԶԻՆԳ» ՎԿ ՓԲԸ Գլխավոր տնօրեն	Աղասի Գասպարյան
«ԱԿԲԱ ԲԱՆԿ» ԲԲԸ, «ԱԿԲԱ ԼԻԶԻՆԳ» ՓԲԸ Խորհրդին կից ռիսկերի կառավարման հանձնաժողովի նախագահ	Աշոտ Կարապետյան

Հաստատող՝

Պաշտոն	Անուն Ազգանուն
«ԱԿԲԱ ԲԱՆԿ» ԲԲԸ Խորհրդի նախագահ «ԱԿԲԱ ԼԻԶԻՆԳ» ՎԿ ՓԲԸ Խորհրդի նախագահ	Սոնա Իշխանյան

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ԲԱԺԻՆ 1. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

1. ՆՊԱՏԱԿԸ ԵՎ ԿԻՐԱՌՄԱՆ ՇՐՋԱՆԱԿԸ

1.1. ԱԿԲԱ ԲԱՆԿԻ ԽՄԲԻ Գաղտնիության քաղաքականությունը (այսուհետ՝ Քաղաքականություն) սահմանում է Խմբում անձնական տվյալների հավաքագրման, մշակման, պահպանման, փոխանցման, ոչնչացման և պաշտպանության, ինչպես նաև բանկային գաղտնիք կազմող տեղեկատվության պահպանման ընդհանուր սկզբունքները:

1.2. Քաղաքականության նպատակն է՝

- Տվյալների պաշտպանության կառավարման հուսալի համակարգի միջոցով պաշտպանել հաճախորդների, աշխատակիցների, Խմբի այլ շահակիցների և Խմբի օրինական շահերը,
- Ապահովել, որ Խումբը գործի կիրառելի ներպետական և միջազգային օրենսդրությամբ սահմանված պահանջներին համապատասխան,
- Սահմանել դերերն ու պատասխանատվության շրջանակը բոլոր այն մարմինների և անձանց համար, ովքեր աջակցում են տվյալների արդյունավետ պաշտպանությանը,
- Սահմանել հստակ սկզբունքներ՝ կարգավորելով Քաղաքականությամբ սահմանված գաղտնի տվյալների որևէ եղանակով օգտագործումը,
- Ապահովել գաղտնիության ռիսկերի նույնականացում և նվազեցում՝ Գաղտնիության ազդեցության գնահատման գործընթացի միջոցով,
- Խմբում խթանել տեղեկատվական անվտանգության մշակույթի պահպանումը և տվյալների անվտանգ ու պատշաճ կառավարումը:

1.3. Քաղաքականությունը հիմք է հանդիսանում Խմբում անձնական տվյալների պաշտպանության և վերահսկողության ապահովման բնագավառում հիմնական լուծումների իրագործման համար: Քաղաքականությունը չի կարող մեկնաբանվել որպես թույլտվություն՝ անձնական տվյալների մշակման կամ բանկային գաղտնիքի տրամադրման կամ բացահայտման համար այն հիմքերով, ծավալով կամ ընթացակարգով, որոնք սահմանված չեն կիրառելի օրենքներով, կարգավորումներով և միջազգային օրենսդրությամբ:

1.4. Քաղաքականությունը կիրառվում է Խմբի ընկերությունների կառավարման բոլոր մակարդակներում, ինչպես նաև բիզնես և ֆունկցիոնալ ստորաբաժանումների աշխատակիցների կողմից: Քաղաքականությունը կիրառելի է նաև բոլոր երրորդ անձանց կողմից, որոնք անձնական տվյալներ են մշակում Խմբի կամ Խմբի ընկերության անունից կամ հասանելիություն ունեն բանկային գաղտնիք կազմող տեղեկատվությանը:

2. ՍԱՀՄԱՆՈՒՄՆԵՐ ԵՎ ՀԱՍԿԱՑՈՒԹՅՈՒՆՆԵՐ

ԱԿԲԱ ԲԱՆԿԻ ԽՈՒՄԲ կամ Խումբ՝ ներառում է Հիմնական ընկերությունը և Դուստր ընկերությունը

Հիմնական ընկերություն կամ Բանկ՝ «ԱԿԲԱ ԲԱՆԿ» ԲԲԸ՝ Խմբի կառավարման հիմնական մարմին

Դուստր ընկերություն կամ Լիզինգ՝ «ԱԿԲԱ ԼԻԶԻՆԳ» ՎԿ ՓԲԸ կամ ցանկացած այլ ընկերություն, որը Հիմնական Ընկերությունն ապագայում կարող է ձեռք բերել կամ հիմնադրել որպես դուստր ընկերություն՝ կիրառելի օրենսդրությամբ սահմանված կարգով:

Հիմնական ընկերության Խորհուրդ՝ Հիմնական ընկերության կոլեգիալ կառավարման մարմինը, որը ՀՀ օրենսդրությամբ և Հիմնական ընկերության կանոնադրությամբ սահմանված իրավասությունների շրջանակում պատասխանատու է Հիմնական ընկերության ռազմավարական վերահսկողության, գործադիր կառավարման վերահսկման և բաժնետերերի և այլ շահակիցների շահերի պաշտպանության համար:

Դուստր ընկերության Խորհուրդ՝ Դուստր ընկերության կոլեգիալ կառավարման մարմինը, որը ՀՀ օրենսդրությամբ և Դուստր ընկերության կանոնադրությամբ սահմանված իրավասությունների շրջանակում պատասխանատու է Դուստր ընկերության ռազմավարական վերահսկողության, գործադիր կառավարման վերահսկման և բաժնետերերի և այլ շահակիցների շահերի պաշտպանության համար:

Խորհուրդ՝ Հիմնական ընկերության խորհուրդը և Դուստր ընկերության խորհուրդը:

Խորհրդին կից հանձնաժողով(ներ)՝ Հիմնական ընկերության խորհրդին և Դուստր ընկերության խորհրդին կից հանձնաժողովները, որոնց նպատակն է աջակցել Հիմնական ընկերության և Դուստր ընկերության խորհուրդներին իրենց պարտականությունների իրականացման գործում:

Քաղաքականության համատեքստում Խորհրդին կից հանձնաժողով(ներ)ը վերաբերում է Խորհրդին կից Ռիսկերի կառավարման հանձնաժողովին:

Հիմնական ընկերության գլխավոր գործադիր տնօրեն (ԳԳՏ) կամ Գլխավոր գործադիր տնօրեն՝ Հիմնական ընկերության միանձնյա գործադիր մարմինը, որը պատասխանատու է Հիմնական ընկերության գործադիր կառավարման և ամենօրյա գործունեության ղեկավարման/վերահսկողության համար՝ գործող օրենսդրությամբ և Հիմնական ընկերության կանոնադրությամբ սահմանված կարգով:

Գլխավոր գործադիր տնօրենին կից հանձնաժողովներ՝ Հիմնական ընկերության գլխավոր գործադիր տնօրենին կից հանձնաժողովներ, որոնք իրականացնում են խորհրդատվական գործառույթներ: Գլխավոր գործադիր տնօրենին կից հանձնաժողովների որոշումները կայացվում են հանձնաժողովի նախագահի՝ Հիմնական ընկերության ԳԳՏ-ի կողմից՝ միանձնյա: Գլխավոր գործադիր տնօրենին կից հանձնաժողովների անդամների կարծիքները խորհրդատվական բնույթ են կրում:

Քաղաքականության համատեքստում Գլխավոր գործադիր տնօրենին կից հանձնաժողովը Համապատասխանության հանձնաժողովն է:

Ավագ ղեկավարություն՝ Հիմնական ընկերության գլխավոր գործադիր տնօրենը, տնօրենները և գլխավոր հաշվապահը:

Բիզնես **ստորաբաժանումներ՝** Խմբի համապատասխան մասնագիտացում ունեցող աշխատողներից կազմված ռեսուրս կենտրոններ, որոնք գործում են որպես ամբողջական բիզնես ուղղություններ: Այս ստորաբաժանումներն ընդգրկում են թե՛ պրոդուկտի/ծառայության ստեղծման, թե՛ վաճառքի մասնագետներ, որոնք պատասխանատու են բիզնես գործընթացի բոլոր փուլերի համար՝ սկսած պրոդուկտի/ծառայության մշակումից մինչև դրա գործարկում, սպասարկում և պլանավորված վերջնարդյունքի ապահովում: Բիզնես ստորաբաժանումներն ընդգրկում են Հիմնական ընկերության հետևյալ երկու բիզնես ուղղությունները (կառուցվածքային ստորաբաժանումները)՝ Մանրածախ բիզնեսի տնօրինությունը և ՓՄՁ և Կորպորատիվ բիզնեսի տնօրինությունը, ինչպես նաև Դուստր ընկերության աշխատողները և ստորաբաժանումները.

Ֆունկցիոնալ ստորաբաժանումներ՝ Խմբի համապատասխան մասնագիտացում ունեցող աշխատողներից կազմված օժանդակող կենտրոններ, որոնք իրականացնում են մասնագիտական, ռազմավարական, կարգավորող օժանդակություն և գործառնական սպասարկում կամ վերահսկողություն բոլոր Բիզնես ստորաբաժանումներին: Ֆունկցիոնալ ստորաբաժանումները ներառում են Հիմնական ընկերության հետևյալ կառուցվածքային ստորաբաժանումները՝ Թվային պլատֆորմների և տեխնոլոգիաների տնօրինությունը, Գործառնական տնօրինությունը, Ֆինանսական տնօրինությունը, Ռիսկերի կառավարման տնօրինությունը, Վարկային կոմիտեների և վերլուծությունների տնօրինությունը, Իրավաբանական և համապատասխանության տնօրինությունը, ՄՌԿ և կազմակերպական զարգացման տնօրինությունը, ՓԼ/ԱՖ դեմ պայքարի և սանկցիաների տնօրինությունը, Տեղեկատվական անվտանգության և կիբեռանվտանգության տնօրինությունը, ինչպես նաև Դուստր ընկերության ՓԼ/ԱՖ դեմ պայքարի և սանկցիաների պատասխանատուն.

Գաղտնի տվյալներ՝ Քաղաքականության իմաստով գաղտնի տվյալներ են համարվում անձնական տվյալները և բանկային գաղտնիք կազմող տեղեկատվությունը:

Հաճախորդ՝ Հիմնական և Դուստր ընկերության հետ գործարար հարաբերություն հաստատող կամ այդպիսի հարաբերությունների մեջ գտնվող անձ, ինչպես նաև անձ, որը Հիմնական և/կամ Դուստր ընկերությանը առաջարկում է կատարել կամ կատարում է մեկանգամյա գործարք.

Անձնական տվյալներ՝ ֆիզիկական անձին վերաբերող ցանկացած տեղեկատվություն, որը թույլ է տալիս կամ կարող է թույլ տալ ուղղակի կամ անուղղակի կերպով նույնականացնել անձի ինքնությունը.

Անձնական տվյալների սուբյեկտ՝ հաճախորդ, այդ թվում՝ իրավաբանական անձի ֆիզիկական անձ ներկայացուցիչ, լիազորված անձ/իրական շահառու, հաճախորդի հետ փոխկապակցված ֆիզիկական անձ, ինչպես նաև երրորդ անձ, ում տվյալները հավաքագրվում են Հիմնական և/կամ Դուստր ընկերության կողմից, Խմբի աշխատակից, նրա հետ փոխկապակցված անձ կամ Խմբի/Խմբի ընկերության հետ փոխկապակցված անձ, դիմորդ.

Անձնական տվյալների ցանկ՝ տվյալների ցանկ, որը վերաբերում է տվյալ սուբյեկտին.

Անձնական տվյալների գաղտնիության պահպանման պահանջներ՝ հաստատված կանոններ, որոնք որոշում են անձնական տվյալների հասանելիության, փոխանցման, տրամադրման և պահպանման պայմանների սահմանափակումները.

Խմբի համապատասխանության գործառույթի պատասխանատու(ներ)՝ Հիմնական ընկերության Համապատասխանության բաժնի պետը և Իրավաբանական և համապատասխանության տնօրենը.

Անձնական տվյալների պաշտպանության պատասխանատու՝ Խմբի աշխատակից, ով վերահսկում և ձեռնարկում է իրավական, կազմակերպչական և տեխնիկական միջոցառումներ Քաղաքականության պահանջներին համապատասխան Խմբում անձնական տվյալների մշակման կազմակերպման գործառույթների պատշաճ կատարումն ապահովելու համար: Խմբում անձնական տվյալների պաշտպանության պատասխանատու է հանդիսանում Համապատասխանության բաժնի պետը.

Անձնական տվյալների հավաքագրում՝ տվյալների սուբյեկտներից անձնական տվյալներ ստանալու ընթացակարգ.

Անձնական տվյալների մշակում՝ գործողություններ անձնական տվյալների հետ, ներառյալ՝ հավաքագրում, համակարգում, կուտակում, պահպանում, հստակեցում (թարմացում, փոփոխություն), օգտագործում, բաշխում (ներառյալ՝ փոխանցում), անձնազերծում, անձնական տվյալների ոչնչացում.

Անձնական տվյալների սուբյեկտի համաձայնություն՝ սույն Կարգով նախատեսված ձևով, անձի կամքի ազատ, հատուկ, անվերապահ և գիտակցված արտահայտում, համաձայն որի սուբյեկտը տեղեկացնում է իր անձնական տվյալների մշակման վերաբերյալ իր համաձայնության մասին.

Անձնական տվյալների փոխանցում՝ Խմբի ընկերության կողմից անձնական տվյալների տրամադրումը երրորդ անձանց՝ տվյալները որոշակի կամ անորոշ շրջանակի այլ անձանց փոխանցելուն կամ դրանց հետ ծանոթացնելուն ուղղված գործողություն, այդ թվում՝ զանգվածային լրատվության միջոցներով անձնական տվյալները հրապարակելը, տեղեկատվական հաղորդակցման ցանցերում տեղադրելը կամ այլ եղանակով անձնական տվյալներն այլ անձի մատչելի դարձնելը.

Անձնական տվյալների արգելափակում՝ անձնական տվյալների փոխանցման, հստակեցման, օգտագործման և ոչնչացման ժամանակավոր կասեցում.

Անձնական տվյալների ոչնչացում (ջնջում)՝ գործողություններ, որոնց արդյունքում անհնար է դառնում վերականգնել անձնական տվյալների բովանդակությունն անձնական տվյալների տեղեկատվական համակարգում և/կամ, որի արդյունքում ոչնչացվում են անձնական տվյալների նյութական կրիչները.

Անձնական տվյալների անձնազերծում՝ գործողություններ, որոնց արդյունքում անհնար է դառնում որոշել սուբյեկտի անձնական տվյալների պատկանելությունն առանց հավելյալ տեղեկատվության օգտագործման.

Անձնական տվյալների տեղեկատվական համակարգ՝ տվյալների բազաներում պարունակվող անձնական տվյալների և դրանց մշակումը ապահովող տեղեկատվական տեխնոլոգիաների և տեխնիկական միջոցների ամբողջություն.

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.

Հանրամատչելի անձնական տվյալներ՝ 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.

GDPR (General Data Protection Regulation)/ անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգ՝ Եվրամիության կանոնակարգով ընդունված անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգ, որի նպատակն է Եվրամիության ռեզիդենտ հանդիսացող տվյալների սուբյեկտների համար ապահովել իրենց անձնական տվյալները վերահսկելու հնարավորություն.

Շահագրգիռ անձ՝ հաճախորդ, գործընկեր, գործակալ, խորհրդատու, կապալառու, մատակարար և վաճառող, միջնորդ, ծառայություններ մատուցող և այլ անձինք, ովքեր կատարում են նմանատիպ առաջադրանքներ կամ գործառույթներ, ինչպես նաև ՀՀ պետական մարմինները և ՀՀ կենտրոնական բանկը.

Լիազոր մարմին՝ ՀՀ կենտրոնական բանկ և/կամ ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալություն:

Գաղտնիության ազդեցության գնահատում՝ գործընթաց՝ ուղղված անձնական տվյալների մշակման նոր կամ էապես փոփոխված գործողություններից/գործընթացներից բխող գաղտնիության ռիսկերի բացահայտմանը, գնահատմանը և մեղմմանը: Գաղտնիության ազդեցության գնահատման նպատակն է գնահատել տվյալների մշակման անհրաժեշտությունն ու համաչափությունը, բացահայտել տվյալների սուբյեկտների իրավունքների և ազատությունների համար առկա ռիսկերը և փաստաթղթավորել այդ ռիսկերի հասցեագրման համար ընդունված հսկողական մեխանիզմները:

Բարձր ռիսկային տվյալների մշակում՝ Անձնական տվյալների մշակում, որը կարող է հանգեցնել ֆիզիկական անձանց իրավունքների և ազատությունների բարձր ռիսկի, ներառյալ՝ անձնական տվյալների հատուկ կատեգորիաների լայնածավալ մշակումը, զգալի իրավական հետևանքներ ունեցող համակարգված ավտոմատացված որոշումների կայացումը: Բարձր ռիսկայնության մշակումը պահանջում է պարտադիր Գաղտնիության ազդեցության գնահատման իրականացում նախքան գործընթացի մեկնարկը:

Անձնական տվյալների մշակման խախտում՝ Միջադեպ, որը հանգեցնում է Խմբի կողմից փոխանցվող, պահվող կամ այլ կերպ մշակվող անձնական տվյալների պատահական կամ անօրինական ոչնչացմանը, կորստին, փոփոխմանը, չարտոնված բացահայտմանը կամ հասանելիությանը:

Բանկային գաղտնիք՝ Բանկի հաճախորդին սպասարկելու կապակցությամբ Բանկին հայտնի դարձած հաճախորդի հաշիվների վերաբերյալ տեղեկությունները, հաճախորդի հանձնարարությամբ կամ հօգուտ հաճախորդի կատարված գործառնությունների վերաբերյալ տեղեկությունները, ինչպես նաև նրա առևտրային գաղտնիքը, գործունեության ցանկացած ծրագրի կամ մշակման, գյուտի, արդյունաբերական նմուշի մասին տեղեկությունները և նրա վերաբերյալ ցանկացած այլ տեղեկություն, որը հաճախորդը մտադիր է եղել գաղտնի պահել, և Բանկը տեղյակ է կամ կարող էր տեղյակ լինել այդ մտադրության վերաբերյալ:

Բանկային գաղտնիքի հրապարակում՝ Բանկային գաղտնիք կազմող տեղեկությունները բանավոր կամ գրավոր ձևով զանգվածային լրատվության միջոցներով կամ այլ կերպ հրապարակելը կամ տարածելը, երրորդ անձին կամ անձանց հայտնի դարձնելը, երրորդ անձանց նման տեղեկություններ հայթայթելու հնարավորություն ուղղակիորեն կամ անուղղակի ընձեռելը, այն է՝ թույլատրելը, չխոչընդոտելը կամ նման տեղեկությունների պահպանման կարգի խախտման հետևանքով այն հնարավոր դարձնելը,

բացառությամբ «Բանկերի և բանկային գործունեության մասին» ՀՀ օրենքի 43 հոդվածով սահմանված դեպքերի: Երրորդ անձ են համարվում բացի Բանկից և իր հաճախորդից, բոլոր այլ անձինք, ընդ որում, Կենտրոնական բանկը, բանկերը և «Վարկային կազմակերպությունների մասին» ՀՀ օրենքով սահմանված վարկային կազմակերպությունները, «Վարկային տեղեկատվության շրջանառության և վարկային բյուրոների գործունեության մասին» ՀՀ օրենքով սահմանված վարկային բյուրոները, Ավանդների հատուցման երաշխավորման հիմնադրամը «Ֆիզիկական անձանց բանկային ավանդների հատուցումը երաշխավորելու մասին» ՀՀ օրենքով սահմանված դեպքերում, երրորդ անձ չեն հանդիսանում:

Բանկային գաղտնիքի տրամադրում՝ Բանկային գաղտնիք կազմող տեղեկությունների տրամադրումը՝ միայն օրենքով սահմանված դեպքերում, հիմքերով և պետական մարմիններին, պաշտոնատար անձանց ու քաղաքացիներին այդ տեղեկությունները բանավոր կամ գրավոր ձևով հաղորդելն է:

3. ՊԱՏԱՍԽԱՆԱՏՈՒ ՄԱՐՄԻՆՆԵՐ ԵՎ ԱՆՁԻՆՔ

3.1. ***Խորհուրդը.***

- Հաստատում է Քաղաքականությունը և դրա էական փոփոխությունները և ապահովում է ընդհանուր վերահսկողություն Քաղաքականության պահանջների պատշաճ իրականացման նկատմամբ:

3.2. ***Խորհրդին կից հանձնաժողով(ներ)ը.***

- Հետևում է Քաղաքականության իրականացմանը և աջակցում է Խորհրդին՝ դրա պահանջների պահպանումն ապահովելու հարցում,
- Զեկուցում է Խորհրդին Քաղաքականության պահանջների համապատասխանության վերաբերյալ:

3.3. ***Գլխավոր գործադիր տնօրենը.***

- Ղեկավարում և ապահովում է Քաղաքականության մշակումը, իրականացումը և արդյունավետ կատարումը Խմբում,
- Ապահովում է, որ Բանկի ներքին ընթացակարգերը համապատասխանեն կարգավորող պահանջներին,
- Աջակցում է Դուստր ընկերության գլխավոր տնօրենին անձնական տվյալների պաշտպանության և բանկային գաղտնիքի պահպանման միասնական մոտեցումներ սահմանելու և կիրառելու հարցում՝ ապահովելով համապատասխանությունը Խմբի ընդհանուր ռազմավարության հետ:

3.4. ***Դուստր ընկերության գլխավոր տնօրենը.***

- Ապահովում է Քաղաքականության պահանջների ներդնումը և ամենօրյա իրականացումը Դուստր ընկերությունում,
- Ապահովում է Հիմնական ընկերության կողմից սահմանված քաղաքականության դրույթների, ինչպես նաև մեթոդաբանությունների պահպանումը:

3.5. ***Խմբի Համապատասխանության գործառույթի պատասխանատուն.***

- Մշակում է Քաղաքականությունը և պատասխանատու է Քաղաքականության կիրառման համար,
- սահմանված պարբերականությամբ Գլխավոր գործադիր տնօրենին, Դուստր ընկերության գլխավոր տնօրենին, Խորհրդին կից հանձնաժողովին և Խորհրդին ներկայացնում է համապատասխան հաշվետվություններ:

3.6. ***Անձնական տվյալների պաշտպանության պատասխանատուն.***

- Գործում է անկախ և տվյալների պաշտպանության բոլոր հարցերի վերաբերյալ հաշվետու է անմիջապես Խորհրդին և Գլխավոր գործադիր տնօրենին/ Դուստր ընկերության գլխավոր տնօրենին:

- Հանդես է գալիս որպես կոնտակտային անձ Լիազոր մարմնի կամ այլ կարգավորողների, ինչպես նաև անձնական տվյալների սուբյեկտների համար:
- «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքով սահմանված դեպքերում Լիազոր մարմնին ծանուցում է տվյալներ մշակելու մտադրության մասին:
- վարում է անձնական տվյալների և բանկային գաղտնիքի հետ կապված միջադեպերի գրանցամատյանները,
- բիզնես և ֆունկցիոնալ ստորաբաժանումներին տրամադրում է համապատասխան խորհրդատվություն Քաղաքականության պահանջների պահպանման վերաբերյալ,
- համակարգում և վարում է Գաղտնիության ազդեցության գնահատման գործընթացը:

3.7. ***Տեղեկատվական անվտանգության և կիբեռանվտանգության տնօրինությունը.***

- ապահովում է տեղեկատվական համակարգերի և տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը:
- Նույնականացնում և գնահատում է տեղեկատվական համակարգերում գաղտնի տվյալների մշակման ընթացքում առաջացող հնարավոր խոցելիությունները և դրանց վերաբերյալ հնարավոր կիբեռսպառնալիքները:
- Ժամանակին հայտնաբերում, արձանագրում և տեղեկացնում է գաղտնի տվյալների անվտանգության հետ կապված կիբեռմիջադեպերի մասին Համապատասխանության բաժնին:

3.8. ***Մարդկային ռեսուրսների կառավարման և կազմակերպական զարգացման տնօրինությունը.***

- Ապահովում է Խմբում թափուր աշխատատեղերի համար դիմած թեկնածուների, աշխատակիցների անձնական տվյալների հավաքագրումը և մշակումը կիրառելի օրենքներին, կարգավորումներին, Քաղաքականությանը և Խմբի այլ ներքին իրավական ակտերին համապատասխան:
- Վարում է աշխատակիցների անձնական տվյալների համապատասխան հաշվառման մատյաններ և ապահովում է դրանց ամբողջականությունը և անվտանգությունը:

3.9. ***Բոլոր աշխատակիցները և ներգրավված անձինք.***

- Պահպանում են Քաղաքականության և կիրառելի օրենքների, կարգավորումների, ներքին իրավական ակտերի պահանջները:

ԲԱԺԻՆ 2. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅՈՒՆ

4. ՇԱՀԱԳՐԳԻՌ ԱՆՁԱՆՑ ՀԵՏ ՀԱՐԱԲԵՐՈՒԹՅՈՒՆՆԵՐԸ

4.1. Անձնական տվյալների պաշտպանության բնագավառում Խումբը իրականացնում է աշխատանքներ շահագրգիռ անձանց պահանջները բացահայտելու և բավարարելու նպատակով: Այդ աշխատանքների շրջանակում Խումբը.

1) պահպանում է հաճախորդների, գործընկերների և մատակարարների (ներառյալ՝ անձնական տվյալները վերահսկող և մշակող կազմակերպությունների) հետ համաձայնագրերի շրջանակներում տրամադրված ամբողջ տեղեկատվությունը, որը կարող է պարունակել ֆինանսական, առևտրային, անձնական և այլ գաղտնի տվյալներ:

2) կրում է պատասխանատվություն շահագրգիռ անձանց գաղտնի տեղեկատվության պահպանման և չտարածման համար, ինչը ենթադրում է ֆինանսական և իրավական պարտավորություններ,

3) ապահովում է, որ տրամադրված տեղեկատվությունը չհրապարակվի երրորդ անձանց՝ առանց շահագրգիռ անձանց կամ պետական իրավասու մարմինների թույլտվության,

4) օրենսդրությամբ, ինչպես նաև ներքին իրավական ակտերով սահմանված կարգով բոլոր շահագրգիռ անձանց տեղեկացնում է իրենց վերաբերյալ տեղեկատվության անվտանգության

պահանջների ապահովման ոլորտում էական փոփոխությունների և գոյացած խնդիրների մասին, որոնց մասին նրանց իրազեկելը Խմբի ընկերությունը համարում է նպատակահարմար և անհրաժեշտ,

5) ապահովում է գործունեության անընդհատությունը շահագրգիռ անձանց հանդեպ իր պարտականությունները կատարելու համար:

4.2.Իրենց հերթին բոլոր շահագրգիռ անձինք պարտավորվում են ապահովել առևտրային գաղտնիքի, հեղինակային իրավունքի պահպանման և Խմբի տեղեկատվության դասակարգման ընթացակարգերի իրականացումը՝ համապատասխան պայմանագրերի հիման վրա:

5. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ՍԿԶԲՈՒՆՔՆԵՐԸ

5.1. **Օրինականության, արդարացիության և թափանցիկության սկզբունք**. Անձնական տվյալները պետք է մշակվեն օրինական, արդարացի և տվյալների սուբյեկտի համար թափանցիկ եղանակով: Մշակումը չպետք է իրականացվի մոլորեցնող, հարկադրական եղանակով կամ այնպիսի ձևով, որը տվյալների սուբյեկտը ողջամտորեն չէր կարող ակնկալել: Խմբի ընկերությունները պետք է տվյալների սուբյեկտներին տրամադրեն հստակ և մատչելի տեղեկատվություն իրենց տվյալների մշակման վերաբերյալ՝ գաղտնիության մասին ծանուցումների և այլ հաղորդակցությունների միջոցով:

Խմբի ընկերությունները պետք է բացառեն առանց տվյալների սուբյեկտի համաձայնության այլ նպատակով տվյալների մշակումը:

5.2. **Համաչափության սկզբունք**. Անձնական տվյալները պետք է հավաքագրվեն որոշակի, հստակ և օրինական նպատակներով և չպետք է հետագայում մշակվեն այդ նպատակների հետ անհամատեղելի եղանակով: Մշակման նպատակները պետք է հստակ սահմանվեն նախքան հավաքագրումը սկսելը և հաղորդվեն տվյալների սուբյեկտներին: Անձնական տվյալների ցանկացած նոր կամ երկրորդային օգտագործում պետք է գնահատվի սկզբնական նպատակի համատեքստում, իսկ անհամատեղելիության դեպքում պետք է սահմանվի նոր իրավական հիմք կամ ստացվի լրացուցիչ համաձայնություն:

Խումբը պետք է կիրառի գաղտնիություն ըստ նախագծման (Privacy by design) սկզբունքը՝ տվյալների պաշտպանության նկատառումները ներդնելով համակարգերի, գործընթացների, ծառայությունների և պրոդուկտների մեջ նախագծման վաղ փուլից: Լռելյայն գաղտնիությունը (privacy by default) նշանակում է, որ այնտեղ, որտեղ առկա է անձնական տվյալների հավաքագրման և մշակման որևէ ընտրության հնարավորություն, լռելյայն կիրառվում են գաղտնիության պաշտպանության ամենախիստ կարգավորումները, քանի դեռ տվյալների սուբյեկտն ակնհայտորեն այլ ընտրություն չի կատարել:

Եթե նպատակին կարելի է հասնել ապանձնավորված կերպով, ապա պետք է բացառվի տվյալների մշակումը:

5.3. **Հավաստիության սկզբունք**. Անձնական տվյալները պետք է լինեն ճշգրիտ և, անհրաժեշտության դեպքում, թարմացվեն: Խումբը պետք է ձեռնարկի բոլոր ողջամիտ քայլերը ապահովելու համար, որ ոչ ճշգրիտ անձնական տվյալները, հաշվի առնելով դրանց մշակման նպատակները, անհապաղ հեռացվեն կամ ուղղվեն: Խումբը պետք է ներդնի ընթացակարգեր, որոնք հնարավորություն կտան տվյալների սուբյեկտներին ուղղել ոչ ճշգրիտ տվյալները, և պարբերաբար ստուգի իր համակարգերում պահվող տվյալների ճշգրտությունը:

5.4. **Սուբյեկտների նվազագույն ներգրավման սկզբունք**. Խումբը հնարավորության և սուբյեկտի գրավոր համաձայնության դեպքում անհրաժեշտ անձնական տվյալները պետք է հավաքագրի այլ մարմիններից՝ տվյալների սուբյեկտի նվազագույն ներգրավվածությունն ապահովելու համար:

5.5. **Պահպանման սահմանափակման սկզբունք**. Անձնական տվյալները պետք է պահպանվեն այնպիսի ձևով, որը թույլ է տալիս նույնականացնել տվյալների սուբյեկտներին ոչ ավել, քան անհրաժեշտ է այն նպատակների համար, որոնցով մշակվում են տվյալները:

5.6. **Ամբողջականության և գաղտնիության (անվտանգություն) սկզբունք**. Անձնական տվյալները պետք է մշակվեն այնպիսի եղանակով, որն ապահովում է պատշաճ անվտանգություն, ներառյալ պաշտպանությունը չլիազորված հասանելիությունից կամ մշակումից, ինչպես նաև պատահական կորստից,

ոչնչացումից կամ վնասումից՝ կիրառելով համապատասխան տեխնիկական և կազմակերպչական միջոցներ: Խումբը պետք է ներդնի բազմամակարդակ անվտանգության համակարգ, որը ներառում է ֆիզիկական և տեխնիկական հսկողության միջոցներ՝ յուրաքանչյուր մշակման գործողությունից բխող ռիսկին համաչափ:

5.7. **Հաշվետվողականության սկզբունք.** Խումբը, որպես տվյալներ մշակող, պատասխանատու է վերը նշված բոլոր սկզբունքների պահպանման համար և պետք է կարողանա ապացուցել սահմանված սկզբունքներին համապատասխանությունը: Հաշվետվողականության սկզբունքը Խմբից պահանջում է ընդունել և ներդնել տվյալների պաշտպանության ներքին իրավական ակտեր և իրականացնել ազդեցության գնահատումներ:

6. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՀԱՎԱՔԱԳՐՄԱՆ ԵՎ ՄՇԱԿՄԱՆ ՆՊԱՏԱԿՆԵՐԸ

6.1. Հիմնական ընկերությունը և Դուստր ընկերությունը անձնական տվյալները մշակում են հետևյալ գործառույթները, գործառնություններն իրականացնելիս.

1) հաշվետվության ներկայացում պետական վերահսկողական մարմիններին՝ համաձայն ՀՀ գործող օրենսդրության պահանջների,

2) բանկային և լիզինգային գործառնությունների իրականացում,

3) ՓԼ/ԱՖ դեմ պայքարի մասին ՀՀ օրենքի պահանջներին համապատասխանելու շրջանակներում գործողությունների իրականացում,

4) վարկային պատմության վերաբերյալ տվյալների հավաքագրում,

5) աշխատանքային հարաբերությունների կարգավորում (աշխատանքի ընդունում, վերապատրաստում, առաջխաղացում, թափուր աշխատատեղերի թեկնածուների անձնական տվյալների հավաքագրում և մշակում),

6) պայմանագրային հարաբերությունների հաստատում անձնական տվյալների սուբյեկտի (հաճախորդներ, մատակարարներ, կապալառուներ և բիզնես գործընկերներ) հետ՝ բանկային և լիզինգային ծառայություններ մատուցելու, ինչպես նաև տարատեսակ ծառայություններից (ֆինանսական, պատվիրակման, ուսուցման, ապրանքների մատակարարման, նորոգման, շինարարական և այլն) օգտվելու համար:

7. ՏՎՅԱԼՆԵՐԻ ՍՈՒԲՅԵԿՏՆԵՐԻ ԴԱՍԱԿԱՐԳՈՒՄԸ ԵՎ ՄՇԱԿՎՈՂ ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՑԱՆԿԸ

7.1. Հիմնական ընկերությունը և Դուստր ընկերությունը մշակում են իրենց հետ կապված հետևյալ սուբյեկտների անձնական տվյալները.

1) թափուր աշխատատեղերի համար դիմած թեկնածուներ,

2) աշխատողներ (ներառյալ՝ փորձաշրջան, վերապատրաստում անցնող անձինք, ժամանակավոր հիմունքներով կամ որոշ գործառույթների պատվիրակման նպատակով այլ կազմակերպությունների հետ կնքված ծառայությունների պատվիրակման/մատուցման պայմանագրի շրջանակներում վարձված այլ աշխատողներ),

3) աշխատողների հետ փոխկապակցված անձինք, որոնց վերաբերյալ անձնական տեղեկությունները Խմբի ընկերություններին հայտնի են դարձել աշխատակցի հետ աշխատանքային պայմանագիր կնքելու, նրա անձնական տվյալները թարմացնելու, շահերի բախումը վերահսկելու միջոցառումներ իրականացնելու և այլ հանգամանքներում,

4) ֆիզիկական անձ բաժնետերեր,

5) գործընկերներ՝ ֆիզիկական անձինք, իրավաբանական անձանց ներկայացուցիչներ, անհատ ձեռնարկատերեր, անձինք, որոնց հետ կնքվել են պայմանագրեր Խմբի ընկերություններին իր

տնտեսական գործունեության իրականացման համար անհրաժեշտ ծառայությունների մատուցման համար,

6) Խորհրդի անդամներ,

7) հաճախորդներ՝ ֆիզիկական անձինք, անհատ ձեռնարկատերեր, ֆիզիկական և իրավաբանական անձանց ֆիզիկական անձ ներկայացուցիչներ (մասնակիցներ, իրական շահառուներ, հիմնադիրներ, տնօրեն, հաշվապահ, լիազորված անձինք, ստորագրության նմուշով հաստատված անձինք, սնանկության կառավարիչներ, օրինական ներկայացուցիչներ, խնամակալներ, հաճախորդի հետ փոխկապակցված այլ անձինք և այլ ֆիզիկական անձինք):

8) հաճախորդների գործարքների անուղղակի մասնակիցներ (գրավադրված գույքի ներգրավվածությամբ կնքվող գործարքների (գործարար հարաբերությունների) հետ առնչվող անձինք, երաշխավորներ, գրավատուներ, ընտանիքի անդամներ), որոնց գծով հավաքագրվում և մշակվում է անձնական տվյալներ կանխորոշված նպատակի համար:

7.2. Հաճախորդներին սպասարկելիս Հիմնական ընկերությունում և Դուստր ընկերությունում օգտագործվող անձնական տեղեկատվության տիպային ցանկը բաղկացած է հետևյալ տվյալներից.

անուն, ազգանուն, հայրանուն,	ռեզիդենտություն,
սեռ,	կենսական շահերի կենտրոն
ծննդյան ամսաթիվ,	ընտանեկան կարգավիճակ,
ծննդավայր,	հեռախոսահամարներ,
անձը հաստատող փաստաթուղթ,	էլեկտրոնային փոստի հասցե,
անձի լուսանկար անձը հաստատող փաստաթղթում կամ այլ փաստաթղթերում,	աշխատանքի վայր և պաշտոն,
անձը հաստատող փաստաթղթի համար,	գործունեության ոլորտ,
անձը հաստատող փաստաթղթի տրման ամսաթիվ,	աշխատավարձ,
անձը հաստատող փաստաթղթի վավերականության ժամկետ,	աշխատանքային փորձ,
գրանցման հասցե (բնակության հասցե),	բանկային ավտոմատացված համակարգում կիրառվող գաղտնաբառեր:

7.3. Վարկային տարբեր պրոդուկտների ստացման և ծառայությունների մատուցման համար դիմող անձանց սպասարկելու նպատակով Խմբի ընկերությունները լրացուցիչ կարող են մշակել նաև հետևյալ անձնական տվյալները.

1) եկամուտ,
2) վճարունակության մակարդակ,
3) ընթացիկ և նախորդ աշխատավայրերի վերաբերյալ կոնտակտային տվյալներ,
4) տեղեկություններ ընտանիքի անդամների, նրանց եկամուտների վերաբերյալ,
5) տեղեկություններ գույքի սեփականության իրավունքի վերաբերյալ,
6) տեղեկություններ պարտավորությունների մասին:

7.4. Խմբի ընկերությունները կարող են մշակել օրենքով թույլատրվող այլ անձնական տվյալներ այն անձանց համար, ովքեր հանդիսանում են Խմբի ընկերությունների աշխատողներ կամ աշխատանքային պայմանագիր կնքելու նպատակով աշխատանքային ընթացակարգերով անցնող անձինք (թափուր աշխատատեղի դիմորդ, թեկնածու):

8. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՄՇԱԿՄԱՆ ՀԻՄՔԵՐԸ

8.1.Անձնական տվյալների մշակումը թույլատրելի է Անձնական տվյալների սուբյեկտի համաձայնության առկայության դեպքում: Առանց տվյալների սուբյեկտի համաձայնության անձնական տվյալներ կարող են մշակվել, եթե տվյալներ մշակելն ուղղակիորեն նախատեսված է օրենքով: Հանրամատչելի անձնական տվյալների մշակման համար անձնական տվյալների սուբյեկտի համաձայնությունը պարտադիր չէ:

8.2. Համաձայնությունը, կախված գործարքի/գործարար հարաբերության տեսակից, կարող է տրվել Հիմնական և Դուստր ընկերություններում կիրառվող տարբեր փաստաթղթերի միջոցով: Հիմնական և Դուստր ընկերության հաճախորդ հանդիսացող Բանկում բանկային հաշիվ ունեցող անձանցից անձնական տվյալների մշակման վերաբերյալ համաձայնությունը ձեռք է բերվում «Ճանաչիր հաճախորդիդ» հարցաթերթիկների՝ eFO 72-02-10, eFO 72-02-11, միջոցով: Որոշ գործարքների դեպքում՝ «Անձնական տվյալների պաշտպանության մասին» ՀՀ օրենքի համաձայն համաձայնությունը կարող է տրվել բանավոր: Բոլոր դեպքերում անձնական տվյալների սուբյեկտի համաձայնությունը պետք է լինի ակնհայտ և փաստաթղթավորվի:

8.3. Անգործունակ և սահմանափակ գործունակ անձանց, ինչպես նաև մինչև 16 տարեկան անչափահասների դեպքում համաձայնությունը տրվում է տվյալների սուբյեկտի օրինական ներկայացուցչի կողմից:

8.4. Առանց անձի համաձայնության՝ արգելվում է **հատուկ կատեգորիայի անձնական տվյալներ** մշակելը, բացառությամբ, երբ տվյալի մշակումն ուղղակիորեն նախատեսված է օրենքով: Հատուկ կատեգորիայի անձնական տվյալների մշակումն անհապաղ դադարեցվում է, եթե վերացել են տվյալները մշակելու հիմքերը և նպատակը: Հատուկ կատեգորիայի անձնական տվյալների մշակումը համարվում է բարձր ռիսկային տվյալների մշակում և մինչև մշակման սկսելը պարտադիր է իրականացնել Գաղտնիության ազդեցության գնահատում:

9. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՓՈԽԱՆՑՈՒՄԸ

9.1.Անձնական տվյալների փոխանցում է համարվում անձնական բնույթի տեղեկատվության տարածումը հաղորդակցման ուղիներով և/կամ էլեկտրոնային կրիչների միջոցով՝ ինչպես ՀՀ տարածքում, այնպես էլ ՀՀ տարածքից դուրս այլ երկիր:

9.2. Հիմնական ընկերության և Դուստր ընկերության կողմից ՀՀ տարածքում անձնական տվյալները կարող են փոխանցվել.

1) ՀՀ կենտրոնական բանկին,

2) «ԱՔՌԱ Քրեդիտ Ռեփորթինգ» ՓԲԸ-ին,

3) պետական իրավասու մարմիններին (ՀՀ դատարաններ, հետախուզության և հարկային մարմին-ներ)՝ ՀՀ օրենսդրությանը համապատասխան,

4) աուդիտորական կազմակերպությունների ներկայացուցիչներին՝ համաձայն վերջիններիս հետ կնքված պայմանագրերի,

5) այլ անձանց՝ դատարանի որոշման հիման վրա կամ անձնական տվյալների սուբյեկտի գրավոր համաձայնությամբ, այդ թվում՝ Բանկի և վճարային համակարգերի կամ այլ կազմակերպությունների հետ համակարգերի ինտեգրման շրջանակներում:

9.3. Անձնական տվյալների փոխանցման ժամանակ տեղեկատվություն ստացողը պատասխանատու է տեղեկատվության անվտանգության և պաշտպանության պահանջների կատարման, ինչպես նաև այդ տեղեկատվության արտահոսքը կանխելու համար:

9.4. Անձնական տվյալները կարող են այլ երկիր փոխանցվել տվյալների սուբյեկտի համաձայնությամբ, կամ եթե տվյալների փոխանցումը բխում է անձնական տվյալների մշակման նպատակներից և (կամ) անհրաժեշտ է այդ նպատակների իրագործման համար:

9.5. Առանց լիազոր մարմնի թույլտվության անձնական տվյալները կարող են փոխանցվել այլ պետություն, եթե այդ պետությունում ապահովված է անձնական տվյալների պաշտպանության բավարար մակարդակ:

9.6. Անձնական տվյալների պաշտպանության բավարար մակարդակը համարվում է ապահովված, եթե.

1) անձնական տվյալները փոխանցվում են միջազգային պայմանագրերին համապատասխան,
2) անձնական տվյալները փոխանցվում են լիազոր մարմնի կողմից պաշտոնական հրապարակված ցուցակում ընդգրկված որևէ երկիր,
3) անձնական տվյալները կարող են փոխանցվել բավարար պաշտպանության մակարդակ չապահովող պետության տարածք միայն լիազոր մարմնի թույլտվությամբ, եթե անձնական տվյալները փոխանցվում են պայմանագրի հիման վրա, և պայմանագրով նախատեսված են անձնական տվյալների պաշտպանության այնպիսի երաշխիքներ, որոնք լիազոր մարմնի կողմից հաստատվել են որպես բավարար պաշտպանություն ապահովող:

9.7. Անձնական տվյալների պաշտպանության բավարար մակարդակ ունեցող և լիազոր մարմնի կողմից պաշտոնական հրապարակված երկրների ցուցակը սահմանվում է «Անձնական տվյալների պաշտպանության գործակալության պետի որոշումը անձնական տվյալների պաշտպանության բավարար մակարդակն ապահովող պետությունների ցանկը սահմանելու մասին» N ԱՏՊՊ-001/24 որոշմամբ: Նշված որոշմամբ անձնական տվյալների պաշտպանության բավարար մակարդակն ապահովող պետությունների ցանկը ներկայացվում է Հավելված 1-ով:

9.8. Հիմնական ընկերությունը և Դուստր ընկերությունը պետք է կնքի տվյալների մշակման գրավոր պայմանագրեր բոլոր այն երրորդ անձանց հետ, որոնք անձնական տվյալներ են մշակում Հիմնական ընկերության և Դուստր ընկերության անունից:

10. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՊԱՀՊԱՆՈՒՄԸ ԵՎ ՈՉՆՉԱՑՈՒՄԸ

10.1. Հիմնական ընկերությունը և Դուստր ընկերությունը պարտավոր է պահպանել մշակման ընթացքում ձեռքբերված անձնական տվյալները, բիզնես նամակագրությունը, բոլոր փաստաթղթերը, փաստաթղթերի պատճենները, որոնք ձեռք են բերվել հաճախորդի կողմից ներկայացված տվյալների պատշաճ ուսումնասիրության արդյունքում, հաճախորդի հետ գործարար հարաբերության դադարեցումից կամ մեկանգամյա գործարքի իրականացումից հետո Տվյալների պահպանման և արխիվացման ցանկով սահմանված պայմաններին համապատասխան:

10.2. Տեղեկատվական համակարգերում և թղթային եղանակով անձնական տվյալների պահպանումն ու ոչնչացումն իրականացվում են Խմբի ներքին իրավական ակտերի դրույթներին համապատասխան:

10.3. Խմբի ընկերությունների կողմից մշակված անձնական տվյալների ոչնչացումն իրականացվում է այնպես, որ անհնար լինի ճշգրիտ կերպով վերականգնել անձնական տվյալների պարունակությունը տեղեկատվական համակարգում, կամ ոչնչացվում են անձնական տվյալների (փաստաթղթերի) նյութական կրիչները:

10.4. Խմբում կիրառվող թվային հիշողության կրիչների վրա առկա տվյալները, այդ թվում՝ անձնական տվյալներ պարունակող, ոչնչացվում են «ԱԿԲԱ ԲԱՆԿ» ԲԲԸ տվյալների կրիչների օգտագործման ուղեցույցում՝ IN 27-01, նկարագրված դրույթների համաձայն:

10.5. Թղթային եղանակով պահպանվող տեղեկատվության ոչնչացումը կատարվում է թղթի մանրացման միջոցով (առկայության դեպքում օգտագործելով թուղթը մանրացնող հատուկ ապարատային սարքավորումներ):

10.6. Խմբի ընկերությունների հաճախորդի, գործընկերոջ կամ Խմբի ընկերությունների հետ կապված անձանց հետ հարաբերությունների դադարեցման դեպքում Խմբի ընկերությունները կարող են երկարաձգել անձնական տվյալների պահպանումը՝ օրենքով նախատեսված ժամկետներից ավելի երկար ժամկետներով,

եթե դա բխում է Խմբի շահերից և իրականացվում է ծառայությունների մատուցման իր ռազմավարության շրջանակներում:

10.7. Կախված որոշակի սուբյեկտների անձնական տվյալների նպատակներից՝ թույլատրվում է Խմբի ընկերությունների կողմից անձնական տվյալները ոչնչացնելու փոխարեն իրականացնել այդ տվյալների անձնազերծում:

11. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐԻ ՍՈՒԲՅԵԿՏԻ ԻՐԱՎՈՒՆՔՆԵՐԸ

11.1. Անձնական տվյալների սուբյեկտն իրավունք ունի ստանալ տեղեկություններ իր անձնական տվյալների, տվյալները մշակելու, մշակելու հիմքերի և նպատակների, Խմբի ընկերությունների, դրանց գտնվելու վայրի, ինչպես նաև այն անձանց մասին, որոնց կարող են փոխանցվել անձնական տվյալները:

11.2. Տվյալների սուբյեկտն իրավունք ունի ծանոթանալու իր անձնական տվյալներին, պահանջել դրանք ուղղել կամ հեռացնել (անձնազերծել), եթե անձնական տվյալներն ամբողջական կամ ճշգրիտ չեն կամ հնացած են կամ ձեռք են բերվել ապօրինի ճանապարհով կամ դրանք հավաքագրելու համար նպատակներն այլևս արդիական չեն:

11.3. Անձնական տվյալների սուբյեկտը կարող է հետ կանչել Հիմնական ընկերությանը և Դուստր ընկերությանը տված իր համաձայնությունը՝ էլեկտրոնային նամակ ուղարկելով Տվյալների պաշտպանության պատասխանատուին dpo@acba.am էլեկտրոնային հասցեով կամ անձամբ Հիմնական ընկերության ցանկացած մասնաճյուղում կամ Գլխամասային գրասենյակում և Դուստր ընկերության Գլխամասային գրասենյակում դիմում ներկայացնելու միջոցով: Համապատասխան ընկերությունը պետք է հաստատի հետկանչման հարցման ստացումը 5 աշխատանքային օրվա ընթացքում և 30 աշխատանքային օրվա ընթացքում վերջնական որոշում կայացնի: Հետկանչման դեպքում Հիմնական ընկերությունը և Դուստր ընկերությունը պետք է ծանուցեն համապատասխան երրորդ անձանց, որոնց փոխանցվել են տվյալները:

11.4. Անձնական տվյալների սուբյեկտն իրավունք ունի չենթարկվելու բացառապես ավտոմատացված մշակման վրա հիմնված որոշման, որը վերջինիս համար առաջացնում է իրավական կամ այլ էական հետևանքներ, բացառությամբ օրենքով նախատեսված դեպքերի: Այն դեպքերում, երբ Խումբը որոշումներ է կայացնում բացառապես ավտոմատացված մշակման հիման վրա, որոնք զգալի հետևանքներ են առաջացնում տվյալների սուբյեկտի համար, Խումբը պետք է տվյալների հավաքագրման պահին տեղեկացնի տվյալների սուբյեկտին նման ավտոմատացված մշակման առկայության և դրա տրամաբանության մասին, թույլ տա տվյալների սուբյեկտին պահանջել որոշման վերանայում մարդու կողմից և թույլ տա տվյալների սուբյեկտին վիճարկել որոշումը և ներկայացնել իր տեսակետը:

11.5. Իր իրավունքների իրացման նպատակով՝ անձնական տվյալների վերաբերյալ տեղեկություն ստանալու կամ դրանց հետ կապված որևէ գործողություն՝ ուղղում, հեռացում կամ անձնազերծում, կատարելու համար տվյալների սուբյեկտը պարտավոր է հարցում կատարել Խմբի ընկերություններին գրավոր եղանակով: Գրավոր հարցումը կարող է ներկայացվել Հիմնական ընկերության ցանկացած մասնաճյուղում կամ Գլխամասային գրասենյակում և Դուստր ընկերության Գլխամասային գրասենյակում կամ էլեկտրոնային նամակ ուղարկել Տվյալների պաշտպանության պատասխանատուի dpo@acba.am էլեկտրոնային հասցեին:

12. ԱՆՁՆԱԿԱՆ ՏՎՅԱԼՆԵՐ ՄՇԱԿՈՂ ՏԵՂԵԿԱՏՎԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԸ

12.1. Անձնական տվյալների մշակումը Բանկում իրականացվում է ինչպես տեղեկատվական տեխնոլոգիաների միջոցով, այնպես էլ առանց այդպիսի միջոցների օգտագործման և կարող է պահպանվել ինչպես թղթային, այնպես էլ էլեկտրոնային կրիչների վրա: Միևնույն ժամանակ, Բանկը/Լիզինգը կատարում է անձնական տվյալների ավտոմատացված և ոչ ավտոմատացված մշակման բոլոր պահանջները, որոնք

նախատեսված են ՀՀ օրենսդրությամբ և ԵՄ անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգով:

12.2. Խմբում անձնական տվյալների մշակումն իրականացվում է հետևյալ փուլերով.

1) հավաքագրում,
2) ձայնագրում,
3) համակարգում,
4) կուտակում,
5) պահուստավորում,
6) պարզաբանում (թարմացում, փոփոխում),
7) օգտագործում, փոխանցում (տրամադրումն իրականացվում է սույն կարգի 5-րդ գլխում սահմանված ՀՀ օրենսդրությամբ նախատեսված դեպքերում),
8) անձնազերծում,
9) արգելափակում,
10) ջնջում,
11) ոչնչացում:

12.3. Անձնական տվյալները մշակող հիմնական տեղեկատվական համակարգերի դասակարգումը հետևյալն է.

1) գործառնական համակարգեր,
2) տվյալների բազաներ,
3) ծրագրային հավելվածներ,
4) սարքավորումներ (ցանցային և սերվերային սարքավորումներ, տվյալների պահպանման և պահուստային համակարգեր և այլն):

13. ԳԱՂՏՆԻՈՒԹՅԱՆ ԱԶԴԵՑՈՒԹՅԱՆ ԳՆԱՀԱՏՈՒՄ

13.1. Գաղտնիության ազդեցության գնահատման (այսուհետ՝ Գնահատում) նպատակն է բացահայտել, գնահատել և հասցեագրել անձնական տվյալների մշակման գործողություններից բխող գաղտնիության ռիսկերը նախքան այդ գործողությունների մեկնարկը:

13.2. Գնահատման իրականացումը պարտադիր է նախքան հետևյալ գործողություններից/գործընթացներից որևէ մեկի մեկնարկը.

1) Անձնական տվյալների մշակման ցանկացած նոր գործողություն, որը նախկինում չի իրականացվել Խմբի կողմից,
2) Գոյություն ունեցող մշակման գործողության ցանկացած էական փոփոխություն (նպատակ, տվյալների կատեգորիաներ, ծավալ, ստացողներ, պահպանման ժամկետ կամ տեխնիկական համակարգեր),
3) Հատուկ կատեգորիայի անձնական տվյալների ցանկացած մշակում,
4) Ցանկացած բարձր ռիսկային տվյալների մշակման գործողություն, ներառյալ լայնածավալ ավտոմատացված որոշումների կայացումը կամ պրոֆիլավորումը,
5) Անձնական տվյալների մշակում ենթադրող նոր տեխնոլոգիաների կամ համակարգերի ներդրում,
6) Անձնական տվյալների մշակման որևէ գործառույթի պատվիրակում երրորդ անձ հանդիսացող մշակողին:

13.3. Այն դեպքերում, երբ հստակ չէ՝ արդյոք Գնահատում պահանջվում է, թե ոչ, համապատասխան ստորաբաժանումը պետք է խորհրդակցի Համապատասխանության բաժնի հետ՝ Գնահատման անհրաժեշտությունը որոշելու նպատակով:

13.4. Յուրաքանչյուր Գնահատում իրականացվում է Համապատասխանության բաժնի կողմից՝ նախաձեռնող ստորաբաժանման հետ համագործակցելով, և պետք է առնվազն ներառի.

1) Մշակման գործողության նկարագրությունը, դրա նպատակը, իրավական հիմքը, տվյալների կատեգորիաները, սուբյեկտները և պահպանման ժամկետը.
2) Անհրաժեշտություն և համաչափություն. արդյո՞ք մշակումն անհրաժեշտ է նշված նպատակի համար, և արդյո՞ք գոյություն ունեն գաղտնիության տեսանկյունից ավելի քիչ ռիսկեր պարունակող այլընտրանքներ.
3) Ռիսկերի բացահայտում. տվյալների սուբյեկտների իրավունքների իրացման համար առկա ռիսկերի բացահայտում.
4) Ռիսկերի նվազեցում. բացահայտված ռիսկերը հասցեագրող տեխնիկական և կազմակերպչական միջոցառումներ.
5) Հաստատող մարմնի կամ անձի նշում:

13.5. Պարտադիր Գնահատման ենթակա՝ անձնական տվյալների մշակումը չի կարող սկսվել, քանի դեռ Գնահատումն ավարտված չէ և համապատասխան հաստատող մարմինը կամ անձը չի ստորագրել այն:

13.6. Հաստատող մարմինը Ցածր ռիսկի դեպքում՝ Համապատասխանության բաժնի պետն է, Բարձր ռիսկի դեպքում՝ Գլխավոր գործադիր տնօրենը, Շատ բարձր ռիսկի դեպքում՝ Խորհուրդը:

13.7. Յուրաքանչյուր ավարտված Գնահատում պետք է վերանայվի առնվազն երեք տարին մեկ անգամ կամ ավելի վաղ՝ հետևյալ դեպքերում. մշակման գործընթացում էական փոփոխություն, մշակման հետ կապված Անձնական տվյալների խախտում, կիրառելի օրենսդրության փոփոխություն:

13.8. Համապատասխանության բաժինը պետք է վարի Գնահատման գրանցամատյան՝ յուրաքանչյուր Գնահատման համար արձանագրելով նույնականացման եզակի համարը, մեկնարկի և ավարտի ամսաթվերը, նախաձեռնող ստորաբաժանումը, գնահատված մշակման նկարագրությունը, ընդունված վերահսկողական մեխանիզմները, մնացորդային ռիսկը, հաստատման կամ մերժման որոշումը և հաջորդ վերանայման ամսաթիվը: Գնահատման ամփոփագիրը պետք է ներառվի Գործադիր կոմիտեին, Խորհրդին կից հանձնաժողովին և Խորհրդին ներկայացվող եռամսյակային հաշվետվության մեջ:

ԲԱԺԻՆ 3. ԲԱՆԿԱՅԻՆ ԳԱՂՏՆԻՔԻ ՊԱՀՊԱՆՈՒՄ

14. ԸՆԴՀԱՆՈՒՐ ԴՐՈՒՅԹՆԵՐ

14.1. Սույն բաժինը կարգավորում է Հիմնական Ընկերության կողմից բանկային գաղտնիք կազմող տվյալների կառավարման և պաշտպանության պահանջները: «Բանկային գաղտնիքի մասին» ՀՀ օրենքով Բանկային գաղտնիքին վերաբերող կարգավորումները լրացնում են Քաղաքականության անձնական տվյալների պաշտպանության ընդհանուր պահանջները:

15. ԲԱՆԿԱՅԻՆ ԳԱՂՏՆԻՔԻ ՊԱՀՊԱՆՄԱՆ ԱՌՆՉՈՒԹՅԱՄԲ ԲԱՆԿԻ ՊԱՐՏԱԿԱՆՈՒԹՅՈՒՆՆԵՐԸ

15.1. Բանկը պարտավոր է չհրապարակել բանկային գաղտնիք կազմող տեղեկատվությունը առանց հաճախորդի գրավոր համաձայնության, բացառությամբ օրենքով ուղղակիորեն թույլատրված կամ պահանջվող դեպքերի:

15.2. Բանկի բոլոր աշխատակիցները կրում են բանկային գաղտնիքի պահպանման պարտականություն, որը շարունակում է գործել նաև աշխատանքային հարաբերությունների դադարեցումից հետո:

15.3. Բանկային գաղտնիքը կարող է տրամադրվել միայն «Բանկային գաղտնիքի մասին» ՀՀ օրենքով սահմանված դեպքերում և կարգով: Բանկային գաղտնիք կազմող տեղեկատվությունը կարող է տրամադրվել.

1) ՀՀ Կենտրոնական բանկին,
2) Քրեական հետապնդում իրականացնող մարմիններին՝ դատարանի որոշման հիման վրա,
3) Դատարանին՝ համապատասխան որոշման հիման վրա,

4) Ֆինանսական համակարգի հաշտարարին,
5) Հաճախորդի ժառանգներին (իրավահաջորդներին)՝ ժառանգության (իրավահաջորդության) իրավունքները հիմնավորող բավարար փաստաթղթերի տրամադրման դեպքում
6) Հարկային մարմիններին՝ դատարանի համապատասխան որոշման հիման վրա:

15.4. Բանկը ներդնում է պայմանագրային և տեխնիկական պաշտպանության միջոցներ՝ ապահովելու համար, որ երրորդ կողմ հանդիսացող ծառայություն մատուցողները և մշակողները պահպանեն բանկային գաղտնիքի այնպիսի պարտավորություններ, որոնք համարժեք են կիրառելի օրենսդրությամբ սահմանված պահանջներին:

ԲԱԺԻՆ 4. ՏՎՅԱԼՆԵՐԻ ՊԱՇՏՊԱՆՈՒԹՅԱՆ ԱՊԱՀՈՎՈՒՄ

16. ՏԵԽՆԻԿԱԿԱՆ ԵՎ ԿԱԶՄԱԿԵՐՊՉԱԿԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐ

16.1. Քաղաքականությամբ սահմանված տվյալների պաշտպանության ապահովման նպատակով Խումբը ձեռնարկում է հետևյալ տեխնիկական և կազմակերպչական միջոցառումները՝

1) սահմանվում և կիրառվում են համապատասխան անվտանգության միջոցառումներ՝ ուղղված տվյալների գաղտնիության, ամբողջականության և հասանելիության ապահովմանը, տվյալների արտահոսքի կանխարգելմանը, ինչպես նաև տվյալների պահպանմանը և անվտանգ ոչնչացման պահանջների սահմանմանը,

2) բարձր կարևորություն ունեցող տվյալները, այդ թվում՝ անձնական տվյալները, ելնելով իրենց գաղտնիության աստիճանից՝ օգտագործվում, պահպանվում և փոխանակվում են գաղտնագրված եղանակով. գործընթացն իրականացվում է սահմանված գաղտնագրման պահանջների և կանոնների պահպանմամբ,

3) տվյալների ամբողջականության ապահովման նպատակով իրականացվում է տվյալների բազաների պարբերական պահուստային կրկնօրինակում,

4) Սահմանվում է պարտադիր նույնականացում տեղեկատվական համակարգ մուտք գործելու դեպքում՝ գաղտնի տեղեկատվության չարտոնված հասանելիության ռիսկը նվազագույնի հասցնելու համար,

5) իրականացվում են անձնական տվյալներին և բանկային գաղտնիք կազմող տեղեկատվությանը հասանելիություն ունեցող աշխատողների գործողությունների հսկողություն, պարբերական ստուգումներ, ներառյալ՝ ավելցուկային հասանելիությունների բացահայտմանն ուղղված ստուգումները,

6) անձնական տվյալների և բանկային գաղտնիքի հետ կապված բոլոր գործողությունները լոգավորվում են:

7) իրականացնում է տեղեկատվական համակարգերի ներթափանցման թեստավորում և խոցելիությունների հայտնաբերում,

8) իրականացվում է իրադարձությունների և կիբեռմիջադեպերի վերլուծությունն ու կառավարում համաձայն «ԱԿԲԱ ԲԱՆԿ» ԲԲԸ տեղեկատվական անվտանգության միջադեպերի կառավարման ուղեցույցով սահմանված կարգի՝ IN 27-09,

9) անձնական տվյալների մշակման գործընթացում օգտագործվող բոլոր տեղեկատվական համակարգերի համար կիրառվում են ամվտանգության ապահովման համակարգեր,

10) կիրառվում է սահմանափակումներ բանկային գաղտնիք կազմող և անձնական տվյալներ մշակող, պահպանող և փոխանցող տեղեկատվական ենթակառուցվածքի մաս կազմող սերվերային սենյակների մուտքի նկատմամբ՝ համաձայն «ԱԿԲԱ ԲԱՆԿ» ԲԲԸ գաղտնի հանդիսացող տարածքներ մուտք գործելու իրավունք ունեցող անձանց ցանկի՝ LI 100-01,

11) կիրառվում են պարտականությունների տարանջատման սկզբունքները՝ անձնական տվյալների և բանկային գաղտնիք կազմող տեղեկատվության պաշտպանության գործընթացների արդյունավետությունն ապահովելու համար,

12) աշխատանքներ են տարվում տվյալների մշակողների իրազեկվածությունը բարձրացնելու ուղղությամբ անձնական տվյալների և բանկային գաղտնիք կազմող տեղեկատվության պաշտպանությունն ամրապնդելու նպատակով,

13) անձնական տվյալներն ու բանկային գաղտնիք կազմող տեղեկատվությունը էլեկտրոնային կրիչներում պահվում են միայն ծածկագրված տեսքով,

14) Բոլոր աշխատանքային և ծառայությունների մատուցման պայմանագրերում պարտադիր ներառվում են անձնական տվյալների և բանկային գաղտնիք կազմող տեղեկատվության պահպանման վերաբերյալ դրույթներ,

15) Բոլոր երրորդ կողմ հանդիսացող տվյալների մշակող մատակարարների դեպքում իրականացվում է պատշաճ ուսումնասիրություն և վերջիններիս հետ կնքվող պայմանագրերում նախատեսվում են հատուկ դրույթներ տվյալների մշակման վերաբերյալ:

ԲԱԺԻՆ 5. ԽՄԲԻ ԱՇԽԱՏԱԿԻՑՆԵՐԻ ՊԱՐՏԱԿԱՆՈՒԹՅՈՒՆՆԵՐԸ ԵՎ ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ

17.1. Խմբի բոլոր աշխատողները, ովքեր ունեն հասանելիություն անձնական տվյալներին և բանկային գաղտնիք կազմող տեղեկատվությանը՝ պայմանավորված իրենց աշխատանքային պարտականությունների կատարմամբ, աշխատանքային պայմանագրով ստանձնում են նշված տվյալների օգտագործման պարտավորություններ և պատասխանատու են այդ տվյալների գաղտնիության ապահովման համար:

17.2. Եթե Խմբի աշխատողը տեղյակ է անձնական տվյալների և բանկային գաղտնիքի չարտոնված բացահայտման դեպքի/փորձի մասին, կամ Խմբի աշխատակցի վրա ճնշում է գործադրվում այդպիսի տեղեկատվություն ստանալու համար, կամ Խմբի աշխատակցի նկատմամբ այլ գործողություններ են կիրառվում (անձնական տվյալների և բանկային գաղտնիքի ապօրինի ձեռքբերման նպատակով), Խմբի աշխատողը պարտավոր է այդ մասին անհապաղ տեղեկացնել իր անմիջական ղեկավարին և/կամ Համապատասխանության բաժնին և/կամ Անձնական տվյալների պաշտպանության պատասխանատուին՝ dpo@acba.am էլեկտրոնային հասցեին նամակ ուղարկելու միջոցով կամ ազդարարման համակարգի միջոցով՝ Whispli անկախ հարթակում կամ Խմբից դուրս բացված acba.compliance@gmail.com էլեկտրոնային հասցեին ուղարկելով դեպքի մանրամասները:

17.3. Խմբի աշխատանքային կայանների, շարժական կրիչների և թղթային կրիչների վրա տեղակայված անձնական տվյալների մշակման և բանկային գաղտնիք կազմող տեղեկատվության օգտագործման ընթացքում անվտանգության միջոցների պահպանման համար պատասխանատվությունը կրում են Խմբի այն աշխատողները, ովքեր մշակում են այդ տվյալները:

17.4. Նշված պահանջները խախտելու դեպքում աշխատողների նկատմամբ կարող են կիրառվել կարգապահական տույժեր, ընդհուպ մինչև աշխատանքից ազատում, ինչպես նաև օրենսդրությամբ սահմանված այլ պատասխանատվության միջոց:

ԲԱԺԻՆ 6. ՀԱՇՎԵՏՎՈՂԱԿԱՆՈՒԹՅՈՒՆ

18.1. Համապատասխանության բաժինը Գլխավոր գործադիր տնօրենին կից հանձնաժողովին, Խորհրդին կից հանձնաժողովին և Խորհրդին ներկայացնում է հաշվետու ժամանակահատվածում արձանագրված անձնական տվյալներին և բանկային գաղտնիքին առնչվող դեպքերի և զարգացումների վերաբերյալ ամփոփ տեղեկատվություն եռամսյակային հաշվետվության շրջանակում:

ԲԱԺԻՆ 7. ՈՒՍՈՒՑՈՒՄ

19.1. Խումբը կարևորում է շարունակական ուսուցումը որպես անձնական տվյալների և բանկային գաղտնիքի պաշտպանության և գաղտնիությանը վերաբերող ռիսկերի արդյունավետ կառավարման էական նախապայման:

19.2. Իրավաբանական և համապատասխանության տնօրինությունը պատասխանատու է բոլոր աշխատակիցների համար անձնական տվյալների և բանկային գաղտնիքի վերաբերյալ պարբերական վերապատրաստումների/ուսուցման կազմակերպման համար: Այս վերապատրաստումները նպատակ ունեն օգնելու աշխատակիցներին իրազեկ լինել Քաղաքականությամբ սահմանված իրենց պարտականություններին:

19.3. Համապատասխանության բաժինը պետք է մշակի և տարածի ուղեցույցներ, հաճախ տրվող հարցեր (ՀՏՀ), և այլ տեղեկատվական նյութեր՝ Խմբում գաղտնիության քաղաքականության արդյունավետ իրականացման նպատակով:

ՀԱՎԵԼՎԱԾ 1

Անձնական տվյալների պաշտպանության բավարար մակարդակն ապահովող պետությունների ցանկ

Ալբանիայի Հանրապետություն	Ճապոնիա
Ամերիկայի Միացյալ Նահանգներ (կազմակերպություններ)	Մալթայի Հանրապետություն
Անդորրայի Իշխանություն	Մեծ Բրիտանիայի և Հյուսիսային Իռլանդիայի Միացյալ Թագավորություն
Ավստրիայի Հանրապետություն	Մոլդովայի Հանրապետություն
Արգենտինայի Հանրապետություն	Մոնակոյի Իշխանություն
Բելգիայի Թագավորություն	Մոնտենեգրո
Բոսնիա և Հերցեգովինա	Նիդերլանդների Թագավորություն
Բուլղարիայի Հանրապետություն	Նոր Զելանդիա
Գերմանիայի Դաշնային Հանրապետություն	Նորվեգիայի Թագավորություն
Դանիայի Թագավորություն	Շվեդիայի Թագավորություն
Էստոնիայի Հանրապետություն	Շվեյցարիայի Համադաշնություն
Իսլանդիա	Չեխիայի Հանրապետություն
Իռլանդիա	Պորտուգալիայի Հանրապետություն
Իտալիայի Հանրապետություն	Ռումինիա
Իսպանիայի Թագավորություն	Ռուսաստանի Դաշնություն
Իսրայելի Պետություն	Սան Մարինոյի Հանրապետություն
Լատվիայի Հանրապետություն	Սերբիայի Հանրապետություն
Լիխտենշտայնի Իշխանապետություն	Սինգապուրի Հանրապետություն
Լիտվայի Հանրապետություն	Սլովակիայի Հանրապետություն
Լյուքսեմբուրգի Մեծ Դքսություն	Սլովենիայի Հանրապետություն
Լեհաստանի Հանրապետություն	Վրաստան
Խորվաթիայի Հանրապետություն	Ուկրաինա
Կանադա	Ուրուգվայի Արևելյան Հանրապետություն
Կորեայի Հանրապետություն	Ֆինլանդիայի Հանրապետություն
Կիպրոսի Հանրապետություն	Ֆրանսիական Հանրապետություն
Հյուսիսային Մակեդոնիայի Հանրապետություն	
Հունաստանի Հանրապետություն	
Հունգարիա	