Գաղտնիության Քաղաքականություն
«ԼԵՆԴՄԱՐԿ ԿԱՊԻՏԱԼ» ՓԲԸ

1. Նպատակը և կիրառման ոլորտը

1.1. Սույն Գաղտնիության Քաղաքականությունը («Քաղաքականություն») սահմանում է «ԼԵՆԴՄԱՐԿ ԿԱՊԻՏԱԼ» ՓԲԸ-ի («Ընկերություն», «մենք», «մեզ» կամ «մերը») կողմից անձնական տվյալների հավաքագրելու, մշակումն իրականացնելու, պահպանելու և պաշտպանելու հիմնական սկզբունքները, նպատակները և ընթացակարգերը:

1.2. Սույն Քաղաքականությունը կիրառվում է Ընկերության կայքի, բջջային հավելվածի կամ կարգավորված ֆինանսական և ներդրումային ծառայություններ մատուցելու ընթացքում ցանկացած այլ եղանակով հավաքված անձնական տվյալների նկատմամբ:

2. Սահմանումներ

2.1. Սույն Քաղաքականությամբ սահմանված տերմիններն ու սահմանումները ունեն հետևյալ նշանակությունները.

Անձնական տվյալներ	Ֆիզիկական անձին («Տվյալների սուբյեկտ») վերաբերող ցանկացած տեղեկատվություն, այդ թվում՝ իրավաբանական անձ հաճախորդի ներկայացուցիչների, բաժնետերերի, վերջնական շահառուների (UBO) կամ պաշտոնատար անձանց վերաբերյալ տեղեկատվություն, երբ տվյալ անձի ինքնությունը կարող է ուղղակի կամ անուղղակի կերպով նույնականացվել նույնացուցիչի (օրինակ՝ անուն, նույնացման համար, գտնվելու վայրի տվյալներ, առցանց նույնացուցիչ) կամ նրա ինքնությանը վերաբերվող մեկ կամ մի քանի հատկանիշների միջոցով:
Մշակում	Անձնական տվյալների հետ իրականացվող ցանկացած գործողություն կամ գործողությունների խումբ՝ ավտոմատացված կամ ոչ ավտոմատացված եղանակով, ներառյալ՝ հավաքում, ամրագրում, կազմակերպում, համակարգում, պահպանում, հարմարեցում, վերափոխում, վերականգնում, ծանոթացում, օգտագործում, հրապարակում, փոխանցում, տարածում, սահմանափակում, ուղեփակում, ոչնչացում:
Տվյալների սուբյեկտ	Ցանկացած ֆիզիկական անձ, որի անձնական տվյալները մշակվում են Ընկերության կողմից, այդ թվում՝ • ֆիզիկական անձ հաճախորդներ, • իրավաբանական անձ հաճախորդների ներկայացուցիչներ, տնօրեններ, աշխատակիցներ, բաժնետերեր և շահառուներ, • Դիմորդներ, ծառայությունից օգտվողներ և Ընկերության կայքի կամ բջջային հավելվածի այցելուներ
Հաճախորդ	Ցանկացած ֆիզիկական կամ իրավաբանական անձ, որը կնքել է կամ հայտնել է մտադրություն կնքելու պայմանագիր Ընկերության հետ ֆինանսական, ներդրումային կամ հարակից ծառայությունների մատուցման համար: Այն դեպքում, երբ Հաճախորդը իրավաբանական անձ է, Ընկերությունը կարող է

	մշակել նրա ներկայացուցիչների կամ առնչվող ֆիզիկական անձանց անձնական տվյալները՝ **«Ճանաչիր քո հաճախորդին»** սկզբունքի, պայմանագրային պարտավորությունների և համապատասխանության ապահովման նպատակներով:
Տվյալների վերահսկող	«ԼԵՆԴՄԱՐԿ ԿԱՊԻՏԱԼ» ՓԲԸ, որը գրանցված և գործող է Հայաստանի Հանրապետության օրենսդրության համաձայն և որը իր կարգավորված ֆինանսական և ներդրումային գործունեության շրջանակում որոշում է անձնական տվյալների մշակման նպատակներն ու միջոցները՝ որպես տվյալների վերահսկող:
Տվյալների մշակող	Ցանկացած ֆիզիկական կամ իրավաբանական անձ, պետական մարմին, գործակալություն կամ այլ կառույց, որը անձնական տվյալներ է մշակում տվյալների վերահսկողի անունից՝ գրավոր տվյալների մշակման պայմանագրի հիման վրա, որն ապահովում է գաղտնիությունը և կիրառելի տվյալների պաշտպանության օրենսդրությանը համապատասխանությունը:
Երրորդ անձ	Ցանկացած անձ կամ կազմակերպություն, որը չի հանդիսանում տվյալների սուբյեկտ, տվյալների մշակող, տվյալների մշակողի կողմից լիազորված անձ կամ այն անձը, որը տվյալների մշակողի կամ նրա լիազորված անձանց ուղիղ ենթակայության ներքո իրավունք ունի անձնական տվյալներ մշակել:
Համաձայնություն	Հաճախորդի հստակ, տեղեկացված և կամավոր համաձայնությունը, որը տրվում է դրական գործողությամբ և թույլ է տալիս Ընկերությանը հավաքել և օգտագործել նրա անձնական տվյալները որոշակի նպատակներով:
Պրոֆիլավորում	Անձնական տվյալների ավտոմատացված մշակման ցանկացած ձև, որը իրականացվում է տվյալների սուբյեկտի անձնական հատկանիշները գնահատելու, մասնավորապես՝ նրա վարքագիծը, նախասիրությունները, ֆինանսական վստահելիությունը կամ ռիսկային պրոֆիլը վերլուծելու կամ կանխատեսելու նպատակով:
Անձնական տվյալների արտահոսք	Անվտանգության խախտում, որի արդյունքում անձնական տվյալների պատահական կամ անօրինական ոչնչացում, կորուստ, փոփոխում, անօրինական հրապարակում կամ դրանց նկատմամբ անօրինական մուտք է տեղի ունեցել՝ փոխանցման, պահպանման կամ այլ կերպ մշակման ընթացքում:
Հսկողություն իրականացնող մարմին	Հայաստանի Հանրապետության արդարադատության նախարարության ենթակայությամբ գործող Անձնական տվյալների պաշտպանության գործակալությունը կամ որևէ այլ իրավասու տվյալների պաշտպանության մարմին, որն ունի իրավասություն վերահսկելու Ընկերության կողմից տվյալների մշակման գործունեությունը:
«Ճանաչիր քո հաճախորդին» տվյալներ	Նույնականացման և վավերացման տվյալները, որոնք հավաքագրվում են Հայաստանի Հանրապետության «Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին» օրենքի հիման վրա, ներառյալ իրավաբանական անձ

	հաճախորդների շահառուների, ներկայացուցիչների և վերջնական վերահսկող անձանց տվյալները:
ՓԼԱՖ	Փողերի լվացման դեմ և ահաբեկչության ֆինանսավորման դեմ պայքարի իրավական և կարգավորող շրջանակը, ներառյալ՝ Հայաստանի Հանրապետության Կենտրոնական բանկի, Ֆինանսական մոնիթորինգի կենտրոնի և համապատասխան միջազգային չափանիշների (օրինակ՝ FATF) կողմից սահմանված պարտավորությունները:
Cookie-ներ և հետկողմային հսկողության տեխնոլոգիաներ	Օգտատիրոջ սարքում պահվող փոքր տեքստային ֆայլեր կամ համարժեք տեխնոլոգիաներ (օրինակ՝ ծրագրային ապահովման հավաքածուներ, փիքսելներ), որոնք հավաքում են տեղեկատվություն օգտագործման, նույնականացման, նախասիրությունների և համակարգի աշխատանքի ցուցանիշների վերաբերյալ:
Անանունացում / Կեղծանվանում	Անձնական տվյալների այնպիսի վերափոխում, որի արդյունքում տվյալները այլևս չի կարելի ուղղակի կամ անուղղակի կերպով վերագրել որևէ անձի (անանունացում), կամ տվյալների սուբյեկտին հնարավոր է նույնականացնել միայն առանձին պահպանվող լրացուցիչ տեղեկատվության կիրառմամբ (կեղծանվանում):
Տեղեկատվական անվտանգության պատասխանատու	Ընկերության աշխատակից, ով տեղեկատվական անվտանգության ապահովմանը զուգահեռ, վերահսկում է նաև սույն Քաղաքականությանը համապատասխանությունը, տրամադրում է խորհրդատվություն տվյալների պաշտպանության ոլորտում գոյություն ունեցող պարտավորությունների վերաբերյալ և հանդես է գալիս որպես կապող օղակ տվյալների սուբյեկտների և հսկողություն իրականացնող մարմինների համար (համաձայն GDPR-ի 37-րդ հոդվածի): Համաձայն GDPR-ի դրույթների Տեղեկատվական անվտանգության պատասխանատուն միաժամանակ գործում է որպես Ընկերության անձնական տվյալների պաշտպանության պատասխանատու:
Կայք և հեռախոսի հավելված	Ընկերության պաշտոնական թվային հարթակները, որոնց միջոցով Հաճախորդները կարող են օգտվել ֆինանսական և ներդրումային ծառայություններից, կապ հաստատել Ընկերության հետ, ինչպես նաև կառավարել հաշիվներն ու գործարքները, ներառյալ համապատասխան API-ները և ապահով ինտերֆեյսները:
Կիրառելի օրենսդրություն	Ընդհանուր առմամբ՝ Հայաստանի Հանրապետության օրենքները, Հայաստանի Հանրապետության Կենտրոնական բանկի ենթաօրենսդրական ակտերը Անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգը (GDPR), Միացյալ Թագավորության 2018 թվականի Անձնական տվյալների պաշտպանության օրենքը, ինչպես նաև OECD Գաղտնիության ուղեցույցները, որքանով դրանք կիրառելի են Ընկերության միջսահմանային և կարգավորված գործունեության նկատմամբ:

Անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգ կամ GDPR	Անձնական տվյալների պաշտպանության ընդհանուր կանոնակարգ (GDPR) — Եվրոպական խորհրդարանի և Եվրոպական միության խորհրդի 2016 թվականի ապրիլի 27-ի (ԵՄ) 2016/679 կանոնակարգը:
Գործընկեր	Ցանկացած ֆիզիկական/իրավաբանական անձ, որը ներգրավված է Ընկերության կողմից ծառայություններ մատուցելու, գործառույթներ իրականացնելու կամ պայմանագրային պարտավորություններ կատարելու նպատակով, ներառյալ տեխնոլոգիական մատակարարները, պահառուները, միջնորդները կամ մասնագիտական խորհրդատուները:
Շահառու	Ֆիզիկական անձ, որը վերջնականապես տիրապետում է կամ վերահսկում է հաճախորդին, իրավաբանական անձին կամ որևէ կառուցվածք, և/կամ որի անունից իրականացվում է գործարքը կամ գործունեությունը՝ համաձայն Հայաստանի Հանրապետության ՓԼԱՖ օրենսդրության սահմանումների:

3. Մեր կողմից հավաքագրվող տեղեկատվությունը

3.1. Ընկերությունը հավաքագրում և մշակում է Անձնական տվյալներ, որոնք անհրաժեշտ են, համապատասխան և համաչափ՝ իր կարգավորվող ֆինանսական և ներդրումային ծառայությունների օրինական մատուցման, օրենսդրական պարտավորությունների կատարման և անվտանգ ու արդյունավետ գործարար գործունեության պահպանման համար:

3.2. Անձնական տվյալները ստացվում են մի քանի օրինական աղբյուրներից, ներառյալ՝ ուղղակիորեն Հաճախորդներից կամ նրանց լիազորված ներկայացուցիչներից, ավտոմատ կերպով՝ Ընկերության թվային հարթակների միջոցով, ինչպես նաև հաստատված երրորդ անձանցից կամ հանրամատչելի աղբյուրներից, ինչպես նկարագրվում է ստորև:

3.3. Հաճախորդների կողմից տրամադրվող տեղեկատվություն

3.3.1. Երբ Հաճախորդը հաստատում է կամ մտադրվում է հաստատել գործարար հարաբերություն Ընկերության հետ, կարող են հավաքագրվել և մշակվել տեղեկատվության հետևյալ տեսակները.

- Նույնականացման և անձնական տվյալներ. անուն, ազգանուն, հայրանուն (եթե կիրառելի է), ծննդյան ամսաթիվ և վայր, ազգություն, քաղաքացիություն, բնակության կամ գրանցման հասցե:
- Կոնտակտային տվյալներ. հեռախոսահամար, էլեկտրոնային հասցե և կապի նախընտրելի լեզու:
- Նույնականացման և վավերացման տվյալներ. անձնագրի կամ ազգային ID-ի համար, ՀՎՀՀ, տրամադրող մարմին և տրամադրման ամսաթիվ, ինչպես նաև «Ճանաչիր քո հաճախորդին» տվյալներ և/կամ ՓԼԱՖ փաստաթղթեր:
- Ֆինանսական և ներդրումային տվյալներ. բանկային հաշվի տվյալներ, միջոցների և գույքի ծագման աղբյուր, եկամտի մակարդակ, զբաղվածության կարգավիճակ, ներդրումային փորձ, հայտարարված ռիսկային պրոֆիլ և ներդրումային նպատակներ:
- Հաշվի և անվտանգության տվյալներ. մուտքանուն, նույնականացման տվյալներ (օրինակ՝ գաղտնաբառեր, PIN կոդեր, կենսաչափական տվյալներ, եթե կիրառելի է) և հաշվին հասանելիության կամ անվտանգության մեթոդների հետ կապված օգտատիրոջ նախասիրություններ:

3.3.2. Ընկերությունը կարող է հավաքագրել նաև լրացուցիչ աջակցող փաստաթղթեր՝ օրենսդրությամբ և ենթաօրենսդրական ակտերով սահմանված պահանջները բավարարելու համար, ինչպիսիք են բնակության հասցեն հաստատող փաստաթղթերը (կոմունալ վճարումների անդորրագրեր, վարձակալության պայմանագրեր), իրավաբանական անձ հաճախորդների շահառուների վերաբերյալ հայտարարագրերը, ինչպես նաև մասնագիտական վկայականները կամ արտոնագրերը՝ հատուկ ծառայությունների կատեգորիաների համար:

3.4. Ավտոմատ կերպով հավաքագրվող տեղեկատվություն

3.4.1. Երբ Հաճախորդները կամ օգտվողները մուտք են գործում Ընկերության պաշտոնական կայք, հեռախոսի հավելված կամ առցանց հարթակներ, որոշ տեխնիկական և վարքային տեղեկություններ ավտոմատ կերպով հավաքագրվում են գործառնական, վերլուծական և անվտանգության նպատակներով, ներառյալ՝

- Տեխնիկական նույնացուցիչներ. IP հասցե, բրաուզերի տեսակ և տարբերակ, սարքի նույնացուցիչ, օպերացիոն համակարգ, էկրանի լուծաչափ, շարժական ցանցի տվյալներ:
- Օգտագործման և փոխազդեցության տվյալներ. սեսիայի ժամանակագրություն, մուտքի և ելքի գրառումներ, այցելած էջեր, սեղմված հղումներ, ինչպես նաև կայքում կամ հեռախոսի հավելվածում իրականացված օգտատիրոջ գործողություններ:
- Cookie-ներ, ծրագրային ապահովման հավաքածուներ և վեբ վերլուծության գործիքներ. տվյալներ, որոնք հավաքվում են Cookie-ների, ծրագրային ապահովման հավաքածուների և վեբ վերլուծական հարթակների միջոցով՝ ապահովելու անվտանգ աշխատանքը, հիշելու օգտատիրոջ նախասիրությունները և վերահսկելու հարթակի արդյունավետությունը:
- Գեոլոկացիոն տվյալներ. մոտավոր գտնվելու վայրը՝ ստացված IP հասցեից կամ սարքի կարգավորումներից՝ տարածաշրջանային համապատասխանության, խարդախության կանխարգելման և ծառայությունների անհատականացման նպատակներով:

3.4.2. Այս տեղեկատվությունը հնարավորության դեպքում մշակվում է համախմբված կամ կեղծանվանված ձևով և չի օգտագործվում օգտատերերին անհատապես նույնականացնելու համար, բացառությամբ այն դեպքերի, երբ դա անհրաժեշտ է անվտանգության ապահովման, խարդախության հայտնաբերման կամ իրավական համապատասխանության նպատակներով:

3.5. Երրորդ աղբյուրներից ստացված տեղեկատվություն

3.5.1. Ուղղակի հավաքագրումից բացի, Ընկերությունը կարող է ստանալ և հաստատել անձնական տվյալներ արտաքին և օրինական աղբյուրներից, ներառյալ, բայց ոչ սահմանափակվելով հետևյալով.

- Ֆինանսական և վճարային հաստատություններ. թղթակից բանկեր, վճարային գործակալներ և պահառուներ, որոնք ներգրավված են գործարքների իրականացման կամ հաշվարկի գործընթացում:
- Կարգավորող և հսկողություն իրականացնող մարմիններ. պետական, հարկային և իրավապահ մարմիններ, որոնք տեղեկատվություն են տրամադրում օրենսդրական կամ կարգավորող լիազորությունների շրջանակում:
- Նույնականացման, «Ճանաչիր քո հաճախորդին» և ՓԼԱՖ ծառայություններ մատուցող արտաքին կազմակերպություններ. սուբյեկտներ, որոնք իրականացնում են անձի նույնականացում, պատժամիջոցների և ցուցակների ստուգում,

նախապատմության ուսումնասիրություն՝ կիրառելի ՓԼԱՖ օրենսդրությանը համապատասխան: Այս երրորդ անձանցից ստացվող անձնական տվյալները կարող են ներառել նույնականացման և կոնտակտային տվյալներ, «Ճանաչիր քո հաճախորդին» և ՓԼԱՖ տեղեկատվություն (օրինակ՝ պատժամիջոցների ցուցակների տվյալներ), իրավաբանական անձի պաշտոնատար անձանց և շահառուների վերաբերյալ տեղեկություններ, գործարքներին առնչվող տվյալներ, ինչպես նաև այլ տեղեկություններ՝ օրենքով սահմանված պարտավորությունները կատարելու կամ համապատասխան ծառայություններ մատուցելու համար:

- Հանրային տվյալների բազաներ և կազմակերպությունների ռեգիստրներ. աղբյուրներ, որոնք պարունակում են տեղեկություններ ընկերությունների սեփականատերերի, շահառուների կամ մասնագիտական կապերի վերաբերյալ:
- Գործընկերներ և երաշխավորներ. սուբյեկտներ կամ անձինք, որոնք ներկայացնում են Հաճախորդների կամ համագործակցում են Ընկերության հետ՝ համաձայնության կամ օրինական պայմանագրային հարաբերության հիման վրա:

3.5.2. Երրորդ աղբյուրներից ստացված բոլոր տվյալները մշակվում են բացառապես օրինական և նախապես որոշված նպատակներով՝ պահպանելով օրինականության, արդարության և թափանցիկության սկզբունքները և պաշտպանված են համապատասխան տեխնիկական և կազմակերպչական երաշխիքներով:

3.5.3. Երբ Ընկերությունը Անձնական տվյալներ է ստանում Տվյալների սուբյեկտից բացի այլ աղբյուրներից, այն պարտավոր է Տվյալների սուբյեկտին տրամադրել այս Գաղտնիության քաղաքականության մեջ պարունակվող տեղեկատվությունը հնարավորինս շուտ, բայց ոչ ուշ, քան մեկ ամսվա ընթացքում, կամ առաջին հաղորդակցման կամ առաջին հրապարակման պահին՝ կախված այն հանգամանքից, թե որն է տեղի ունենում ավելի շուտ, եթե կիրառելի է բացառություն:

3.6. Ճշգրտություն և պատասխանատվություն

3.6.1. Հաճախորդները պատասխանատու են Ընկերությանը տրամադրված բոլոր Անձնական տվյալների և փաստաթղթերի ճշգրտության, ամբողջականության և արդիականության ապահովման համար:

3.6.2. Ընկերությունը կարող է պարբերաբար պահանջել, որպեսզի Հաճախորդները հաստատեն կամ թարմացնեն իրենց տեղեկատվությունը՝ ապահովելու տվյալների ճշգրտությունը և կիրառելի օրենքներին ու ներքին ընթացակարգերին համապատասխանությունը:

3.7. Անձնական տվյալների պարտադիր տրամադրում

3.7.1. Շատ դեպքերում Ընկերության կողմից պահանջվող անձնական տվյալների տրամադրումը հանդիսանում է օրենսդրությամբ և/կամ պայմանագրով սահմանված պահանջ, որը անհրաժեշտ է՝

- ՓԼԱՖ և այլ կարգավորող պարտավորություններին համապատասխանելու համար, և
- ֆինանսական և ներդրումային ծառայությունների մատուցման համար պայմանագրեր կնքելու և կատարելու նպատակով:

3.7.2. Այն դեպքում, երբ տվյալների սուբյեկտը չի տրամադրում կամ հրաժարվում է տրամադրել անձնական տվյալներ, որոնք պահանջվում են օրենքով կամ պայմանագրով, Ընկերությունը կարող է անկարող լինել հիմնել կամ շարունակել գործարար հարաբերությունը, բացել կամ պահպանել հաշիվը, կատարել գործարքներ կամ մատուցել որոշակի ծառայություններ:

4. Մշակման նպատակները և իրավական հիմքերը

4.1. Ընկերությունը անձնական տվյալները մշակում է միայն որոշված, հստակ և օրինական նպատակներով՝ հիմնվելով GDPR-ի 6-րդ հոդվածում և Հայաստանի Հանրապետության «Անձնական տվյալների պաշտպանության մասին» օրենքում սահմանված առնվազն մեկ իրավական հիմքի վրա:

4.2. Անձնական տվյալները չեն մշակվում այնպիսի նպատակներով, որոնք անհամատեղելի են սկզբնապես սահմանված նպատակների հետ: Ցանկացած նոր կամ լրացուցիչ մշակում ենթակա է տվյալների սուբյեկտին նախնական ծանուցման և՝ անհրաժեշտության դեպքում, վերջինիս հստակ համաձայնության ստացման:

4.3. Անձնական տվյալների մշակման հիմնական նպատակներն ու դրանց համապատասխան իրավական հիմքերը ամփոփված են ստորև.

Մշակման նպատակը	Նկարագրություն	Իրավական հիմք
Հաշվի գրանցում և ծառայությունների մատուցում	Հաճախորդի հաշիվների ստեղծում, կառավարում և պահպանում. ֆինանսական և ներդրումային ծառայություններին հասանելիության ապահովում, պայմանագրային պարտավորությունների կատարում և Հաճախորդի հետ հաղորդակցության կազմակերպում:	Պայմանագրի կատարում
Հաճախորդի նույնականացում և վավերացում («Ճանաչիր քո հաճախորդին» / ՓԼԱՖ)	Հաճախորդի ինքնության, շահառուի և միջոցների ծագման ամբողջական ստուգում. անհրաժեշտ պատշաճ հետաքննության իրականացում և ՓԼԱՖ օրենսդրությամբ ու ՀՀ ԿԲ ենթաօրենսդրական ակտերով սահմանված ստուգումների կատարում:	Օրինական պարտավորություն
Կարգավորող պահանջներին համապատասխանություն և հաշվետվություն	Կարգավորող մարմինների՝ մասնավորապես Հայաստանի Հանրապետության Կենտրոնական բանկի, հարկային մարմինների և այլ իրավասու մարմինների կողմից սահմանված հաշվետվությունների, գրառման, աուդիտի և ստուգումների պահանջներին համապատասխանեցում:	Օրինական պարտավորություն
Գործարքների իրականացում և հաճախորդների աջակցություն	Ֆինանսական գործարքների մշակում, Հաճախորդի հանձնարարականների կատարում, հաշվարկների հաստատում և պաշտոնական հաղորդակցական ուղիներով աջակցություն տրամադրում:	Պայմանագրի կատարում
Խարդախության կանխարգելում, ռիսկերի կառավարում և SS անվտանգություն	Անօրինական մուտքի կանխարգելում, համակարգերի աշխատանքի մոնիթորինգ, խարդախության կամ կասկածելի գործունեության հայտնաբերում, ինչպես նաև Հաճախորդների հաշիվների և Ընկերության համակարգերի ամբողջականության պաշտպանություն: Նշվածը հանդիսանում է Ընկերության օրինական շահ:	Օրինական շահ, Օրինական պարտավորություն

Ծառայության բարելավում և վերլուծություն	Ընկերության հարթակների, ծառայությունների և ներքին գործընթացների գնահատում, բարելավում և օպտիմալացում՝ ամփոփիչ վերլուծությունների և հետադարձ կապի միջոցով՝ ելնելով Ընկերության օրինական շահից:	Օրինական շահ, Համաձայնություն
Մարքեթինգ և հաղորդակցություն	Ծառայությունների թարմացումների, հետազոտական նյութերի կամ գովազդային տեղեկատվություն տարածում, որոնք վերաբերում են Հաճախորդի հետաքրքրություններին և նախասիրություններին	Համաձայնություն, Օրինական շահ
Իրավական պահանջներ և վեճերի կարգավորում	Իրավական պահանջների ներկայացում, պաշտպանություն կամ իրականացում. վեճերի, բողոքների կամ հետաքննությունների վարում և Ընկերության իրավունքների ու գույքի պաշտպանություն, ինչը համարվում է Ընկերության օրինական շահ:	Օրինական շահ; Օրինական պարտավորություն

4.3.1. Թույլատրելի սահմանափակ դեպքերում, և միայն այն դեպքում, երբ դա պահանջվում է ՓԼԱՖ-ի, խարդախության կանխարգելման, սանկցիաների ստուգման կամ այլ կարգավորող նպատակներով, Ընկերությունը կարող է մշակել հատուկ կատեգորիայի անձնական տվյալներ (օրինակ՝ քաղաքական հայացքներ պարզաբանող տվյալներ՝ քաղաքական ազդեցիկ անձանց նույնականացման համատեքստում), ինչպես նաև հանցագործություններին և դատապարտվածությանը վերաբերող անձնական տվյալներ: Այսպիսի մշակումն իրականացվում է GDPR-ի 9(2) և 10-րդ հոդվածներում սահմանված մեկ կամ մի քանի հիմքերի վրա, ներառյալ՝ մասնավորապես, այն դեպքերը, երբ մշակումն անհրաժեշտ է.

- հանրային զգալի շահից ելնելով՝ ԵՄ կամ որևէ անդամ պետության օրենքի հիման վրա (օրինակ՝ ՓԼԱՖ օրենսդրություն և հարակից կարգավորող պահանջներ), կամ
- իրավական պահանջներ ներկայացնելու, պաշտպանելու կամ իրականացնելու համար:

4.4. Ընկերությունը կարող է անձնական տվյալները մշակել նաև երկրորդային կամ համատեղելի նպատակներով, օրինակ՝ ներքին աուդիտի, վիճակագրական վերլուծության և գրառումների պահպանման համար, եթե նման մշակումն համապատասխանում է սկզբնական օրինական հիմքին և չի խախտում տվյալների սուբյեկտի իրավունքներն ու ազատությունները:

4.5. Այն դեպքերում, երբ տվյալների մշակումն իրականացվում է համաձայնության հիման վրա, տվյալների սուբյեկտը իրավունք ունի ցանկացած պահին հետ կանչելու իր համաձայնությունը՝ առանց ազդելու մինչև հետկանչը իրականացված մշակման օրինականության վրա:

4.6. Ընկերությունը չի ընդունում որոշումներ՝ հիմնված բացառապես ավտոմատացված մշակման վրա, այդ թվում՝ պրոֆիլավորման, որոնք իրավական հետևանքներ են առաջացնում տվյալների սուբյեկտի համար կամ նրան նման կերպով զգալիորեն ազդում՝ GDPR-ի 22-րդ հոդվածի իմաստով: Եթե Ընկերությունը ապագայում մտադիր է ներդնել նման ավտոմատացված որոշումների կայացում, այն պետք է Տվյալների սուբյեկտներին տրամադրի հատուկ նախնական ծանուցում և տեղեկատվություն ներգրավված տրամաբանության, ինչպես նաև նման մշակման նշանակության և կանխատեսվող հետևանքների մասին:

5. Տվյալների սուբյեկտի իրավունքները

5.1. Հայաստանի Հանրապետության «Անձնական տվյալների պաշտպանության մասին» օրենքի և GDPR-ի համաձայն՝ յուրաքանչյուր անձ, որի անձնական տվյալները մշակվում են Ընկերության կողմից, ունի հետևյալ իրավունքները՝ կիրառելի իրավական և կարգավորող սահմանափակումների շրջանակում.

- Մուտքի իրավունք. Տվյալների սուբյեկտը ունի իրավունք ստանալու հաստատում այն մասին, թե արդյոք Ընկերությունը մշակում է իրեն վերաբերող անձնական տվյալներ, և եթե այո՝ ստանալու այդ տվյալների պատճենը, ինչպես նաև տեղեկություն մշակման նպատակների, տվյալների կատեգորիաների, տվյալների ստացողների և պահպանման ժամկետների վերաբերյալ:
- Ուղղման իրավունք. Տվյալների սուբյեկտը կարող է պահանջել ոչ ճիշտ կամ ոչ ամբողջական անձնական տվյալների ուղղում կամ լրացում՝ ապահովելու դրանց ճշգրտությունն ու համապատասխանությունը:
- Ջնջման իրավունք («Մոռացության իրավունք»). Տվյալների սուբյեկտը կարող է պահանջել իր անձնական տվյալների ջնջումը, եթե առկա են օրինական հիմքեր, օրինակ՝ համաձայնության հետկանչում, մշակման նպատակի դադարեցում կամ անօրինական մշակում: Այս իրավունքը կարող է սահմանափակվել այն դեպքերում, երբ տվյալների պահպանումը պահանջվում է օրենքով կամ կարգավորող պարտավորություններով (օրինակ՝ ՓԼԱՖ փաստաթղթերի պահպանման պահանջով):
- Մշակման սահմանափակման իրավունք. Տվյալների սուբյեկտը կարող է պահանջել, որ Ընկերությունը ժամանակավորապես դադարեցնի անձնական տվյալների մշակումը որոշակի հանգամանքներում, ներառյալ՝ տվյալների ճշգրտության կամ օրինականության վերաբերյալ վեճերի առկայության դեպքում կամ երբ տվյալները անհրաժեշտ են իրավական պահանջներ ներկայացնելու կամ պաշտպանելու համար:
- Առարկելու իրավունք. Տվյալների սուբյեկտը կարող է առարկել տվյալների մշակման դեմ, երբ այն իրականացվում է Ընկերության օրինական շահերից ելնելով կամ ուղղակի մարքեթինգի նպատակներով: Ընկերությունը պարտավոր է դադարեցնել տվյալների մշակումն, եթե չի ներկայացվում համոզիչ օրինական հիմնավորում կամ շարունակման պարտավորություն՝ օրենքով սահմանված դեպքերում:
- Տվյալների տեղափոխելիության իրավունք. Այն դեպքերում, երբ տվյալների մշակումն իրականացվում է համաձայնության կամ պայմանագրի հիման վրա և ավտոմատացված եղանակով, տվյալների սուբյեկտը կարող է պահանջել ստանալ իր անձնական տվյալները կառուցվածքային, տարածված և մեքենայով ընթեռնելի ձևաչափով, կամ պահանջել դրանց փոխանցումը մեկ այլ տվյալների վերահսկողի՝ տեխնիկական հնարավորության դեպքում:
- Համաձայնության հետկանչման իրավունք. Այն դեպքերում, երբ տվյալների մշակումը հիմնված է համաձայնության վրա, տվյալների սուբյեկտը կարող է ցանկացած պահին հետ կանչել իր համաձայնությունը՝ առանց ազդելու մինչև հետկանչը կատարված մշակման օրինականության վրա: Որոշ ծառայություններ կարող են սահմանափակվել, եթե դրանց մատուցումը պահանջում է որոշակի տվյալների մշակում:
- Բողոք ներկայացնելու իրավունք. Տվյալների սուբյեկտը կարող է բողոք ներկայացնել իր անձնական տվյալների մշակման վերաբերյալ՝ Հայաստանի Հանրապետության արդարադատության նախարարության ենթակայությամբ գործող Անձնական տվյալների պաշտպանության գործակալություն, կամ կիրառելիության դեպքում, Եվրոպական տնտեսական տարածքի որևէ այլ իրավասու հսկողություն իրականացնող մարմին:

5.2. Վերոնշյալ իրավունքներից որևէ մեկի իրականացման վերաբերյալ դիմումները պետք է ներկայացվեն գրավոր կամ էլեկտրոնային ձևով՝ սույն Քաղաքականության 11-րդ բաժնում նշված կոնտակտային տվյալների միջոցով՝ ուղղված Ընկերության Տեղեկատվական անվտանգության պատասխանատուին: Ընկերությունը յուրաքանչյուր պատշաճ դիմում կքննի

և կպատասխանի դրա ստացումից մեկ ամսվա ընթացքում, իսկ այդ ժամկետը կարող է երկարացվել կիրառելի օրենքով սահմանված կարգով, եթե դիմումը լինի հատուկ բարդության կամ մեծաքանակ դիմումների պատճառով:

6. Անձնական տվյալների փոխանցում և հրապարակում

6.1. Ընկերության կողմից մշակվող անձնական տվյալները կարող են հրապարակվել կամ փոխանցվել միայն այն դեպքերում, երբ այդ փոխանցումը անհրաժեշտ, օրինական և համաչափ է պայմանագրային, իրավական կամ կարգավորող պարտավորությունների կատարման համար և միշտ՝ անձնական տվյալների պաշտպանության կիրառելի օրենսդրությանը համապատասխան:

6.2. Ընկերությունը կարող է անձնական տվյալները փոխանցել հետևյալ ստացողներին.

- Կարգավորող և հսկողություն իրականացնող մարմիններ. ներառյալ, բայց չսահմանափակվելով Հայաստանի Հանրապետության Կենտրոնական բանկով (ՀՀ ԿԲ), հարկային մարմիններով, դատական կամ իրավապահ մարմիններով, այն դեպքերում, երբ տվյալների փոխանցումը պահանջվում է օրենքով կամ կարգավորող ակտերով, ստուգումների կամ օրինական հրամանների կատարման նպատակով:
- «Ճանաչիր քո հաճախորդին» և ՓԼԱՖ նույնականացման ծառայություններ մատուցող կազմակերպություններ. հաճախորդի պատշաճ հետազոտության, սանկցիաների ստուգման և շարունակական մոնիթորինգի նպատակով՝ Հայաստանի Հանրապետության «Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին» օրենքին համապատասխան:
- SS և ամպային ենթակառուցվածքների մատակարարներ. որոնք պատասխանատու են Ընկերության տեղեկատվական համակարգերի և թվային հարթակների անվտանգության, հոսթինգի, սպասարկման և գործունեության ապահովման համար՝ խիստ պայմանավորվածությամբ տվյալների պահպանման և գաղտնիության վերաբերյալ:
- Արտաքին աուդիտորներ, իրավաբանական խորհրդատուներ և մասնագիտական խորհրդատուներ. ներգրավված աուդիտի, համապատասխանության կամ իրավական աջակցություն տրամադրելու նպատակով և որոնք պարտավորված են մասնագիտական գաղտնիությամբ և պայմանագրային գաղտնիության դրույթներով:
- Գործընկերներ և երրորդ կողմ ծառայություններ մատուցողներ. որոնք ներգրավված են ֆինանսական կամ ներդրումային ծառայությունների մատուցման գործընթացում և գործում են՝ կիրառելի անձնական տվյալների պաշտպանության օրենսդրությանը համապատասխանող պայմանագրերի հիման վրա, ինչպես նաև՝ անհրաժեշտության դեպքում, Հաճախորդի նախնական համաձայնությամբ:

6.3. Ընկերությունից անձնական տվյալներ ստացող բոլոր երրորդ անձինք պարտավոր են մշակել այդ տվյալները միայն այն նպատակներով, որոնց համար դրանք տրամադրվել են, և Ընկերության գրավոր հրահանգներին, գաղտնիության դրույթներին և կիրառելի օրենսդրությանը համապատասխան:

6.4. Անձնական տվյալները երբեք չեն վաճառվում, վարձակալվում կամ փոխանցվում որևէ երրորդ անձի՝ մարքեթինգային կամ այլ առևտրային նպատակներով, որոնք կապ չունեն Ընկերության օրինական բիզնես գործունեության կամ Հաճախորդներին ծառայություններ մատուցելու հետ:

6.5. Այն դեպքերում, երբ դա պահանջվում է օրենքով կամ սահմանվում է տվյալների փոխանցման միջազգային կանոններով, Ընկերությունը պետք է ապահովի, որ մինչև որևէ միջազգային փոխանցում իրականացնելը առկա լինեն համապատասխան պայմանագրային և տեխնիկական պաշտպանության միջոցներ (օրինակ՝ Ստանդարտ պայմանագրային դրույթներ կամ համարժեք մեխանիզմներ):

7. Տվյալների անվտանգություն

7.1. Ընկերությունը կիրառում և պահպանում է տեխնիկական և կազմակերպչական անվտանգության համապարփակ միջոցներ՝ ապահովելու իր գործունեության շրջանակում մշակվող անձնական տվյալների գաղտնիությունը, ամբողջականությունը և հասանելիությունը: Այս միջոցները մշակված են՝ Հայաստանի Հանրապետության Կենտրոնական բանկի (ՀՀ ԿԲ) պահանջներին, GDPR-ի 32-րդ հոդվածին, Ընկերության տեղեկատվական անվտանգության համակարգի ներքին իրավական ակտերին և կիրառելի միջազգային տեղեկատվական անվտանգության ստանդարտներին համապատասխան:

7.2. Ընկերության տվյալների պաշտպանության շրջանակը ներառում է, սակայն չի սահմանափակվում հետևյալ միջոցներով.

- Գաղտնագրում և ապահով հաղորդակցություն. TLS (Transport Layer Security) և SSL (Secure Socket Layer) արձանագրությունների կիրառում՝ Հաճախորդների և Ընկերության համակարգերի միջև փոխանցվող տվյալների պաշտպանության համար:
- Մուտքի վերահսկում և նույնականացում. դերերի վրա հիմնված մուտքի վերահսկման մեխանիզմների, բազմագործոն նույնականացման (MFA) և օգտատերերի լիազորման ընթացակարգերի կիրառում՝ մուտքը սահմանափակելու միայն լիազորված անձանց համար:
- Համակարգերի մոնիթորինգ և խոցելիությունների ստուգում. ցանցերի և հավելվածների շարունակական մոնիթորինգ, պարբերական ներթափանցման (penetration) թեստավորում և խոցելիությունների գնահատում՝ հնարավոր վտանգները հայտնաբերելու, կանխելու և նվազեցնելու նպատակով:
- Ֆիզիկական և միջավայրային անվտանգություն. տվյալների կենտրոնների և գրասենյակային տարածքների պաշտպանություն՝ վերահսկվող մուտքի համակարգերի, տեսահսկման և միջավայրային ապահովման միջոցներով՝ կանխելու չարտոնագրված մուտքը, տվյալների կորուստը կամ վնասումը:
- Տվյալների պահուստավորում և բիզնեսի շարունակականություն. տվյալների պարբերական պահուստավորում, աղետների վերականգնման պլաններ և կրկնօրինակման մեխանիզմներ՝ ծառայությունների շարունակականությունն ու տեղեկատվության հասանելիությունը ապահովելու նպատակով:
- Տվյալների անվտանգ պահպանում և ոչնչացում. անձնական տվյալների անվտանգ պահպանում՝ գաղտնագրված կամ մուտքի վերահսկմամբ համակարգերում, ինչպես նաև ժամկետը լրացած, ավելորդ կամ օրենքով այլևս չպահանջվող տվյալների անվտանգ ջնջում կամ ոչնչացում՝ ոլորտային լավագույն մեթոդներով:

7.3. Բոլոր աշխատակիցները, պայմանագրային գործընկերները և այն երրորդ անձինք, որոնք լիազորված են հասանելիություն ունենալու անձնական տվյալներին, պարտավոր են պահպանել գաղտնիության պահպանման պարտավորությունները և անցնել տեղեկատվական անվտանգության և տվյալների պաշտպանության սկզբունքների վերաբերյալ ուսուցում՝ Ընկերության համապատասխանության ծրագրի շրջանակում:

7.4. Ընկերությունը պարտավորվում է անհապաղ հետաքննել և արձագանքել ցանկացած տվյալների արտահոսքի կամ անվտանգության միջադեպի, իրականացնել համապատասխան վերականգնողական միջոցներ, ինչպես նաև՝ օրենքով սահմանված դեպքերում, տեղեկացնել իրավասու մարմիններին և տուժած տվյալների սուբյեկտներին:

7.5. Հաճախորդները պատասխանատու են իրենց մուտքային տվյալների, գաղտնաբառերի և նույնականացման տվյալների գաղտնիության պահպանման համար: Ընկերությունը խորհուրդ է տալիս Հաճախորդներին կիրառել հուսալի անվտանգության մեխանիզմներ, ներառյալ՝

եզակի գաղտնաբառերի օգտագործումը և սարքերի անվտանգ կառավարումը, երբ նրանք մուտք են գործում Ընկերության թվային հարթակներ և ծառայություններ:

8. Տվյալների պահպանման ժամկետներ

8.1. Ընկերությունը անձնական տվյալները պահպանելու է միայն այնքան ժամանակ, որքան անհրաժեշտ է այդ տվյալները հավաքելու և մշակելու նպատակները կատարելու համար, կամ այնքան, որքան դա պահանջվում է Հայաստանի Հանրապետության կիրառելի օրենքներով և կարգավորումներով, ներառյալ՝ ՓԼԱՖ պահանջներով:

8.2. Պահպանման ժամկետները որոշվում են հետևյալ չափանիշների հիման վրա.

- անձնական տվյալների բնույթը և կատեգորիան,
- մշակման նպատակն ու իրավական հիմքը,
- Հայաստանի Հանրապետության Կենտրոնական բանկի (ՀՀ ԿԲ), հարկային մարմինների կամ այլ իրավասու մարմինների կողմից սահմանված օրենսդրական կամ կարգավորող պահանջները,
- տեղեկատվության պահպանման անհրաժեշտությունը՝ իրավական պահանջներ ներկայացնելու, իրականացնելու կամ պաշտպանելու նպատակով:

8.3. Ընկերությունը կիրառում է հետևյալ ստանդարտ պահպանման ժամկետները, եթե օրենքով կամ կարգավորող ակտերով այլ ժամկետ չի սահմանված.

- ՓԼԱՖ և «Ճանաչիր քո հաճախորդին» փաստաթղթեր. պահպանվում են առնվազն հինգ (5) տարի՝ գործարար հարաբերությունների ավարտից կամ գործարքի ավարտից հետո՝ համաձայն «Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին» ՀՀ օրենքի:
- Գործարքային, հաշվապահական և աուդիտորական գրառումներ. պահպանվում են յոթ (7) տարի՝ գործարքի կամ գրառման ձևավորման օրվանից՝ ֆինանսական և հարկային կարգավորումների համաձայն:
- Պայմանագրային և նամակագրության գրառումներ. պահպանվում են այնքան ժամանակ, որքան անհրաժեշտ է պայմանագրային հարաբերությունները կառավարելու համար, և մինչև հինգ (5) տարի՝ դրանց ավարտից հետո, եթե վեճերի կարգավորման կամ իրավական պահանջների համար ավելի երկար պահպանում չի պահանջվում:
- Մարքեթինգային և հաղորդակցման նախասիրություններ. պահպանվում են մինչև տվյալների սուբյեկտը հետ կանչի իր համաձայնությունը կամ հրաժարվի նման հաղորդագրություններ ստանալուց:
- Աշխատանքային և ներքին կառավարման գրառումներ. պահպանվում են Ընկերությանը կիրառելի աշխատանքային, հաշվապահական և համապատասխանության պարտավորություններին համապատասխան:

8.4. Կիրառելի պահպանման ժամկետի ավարտին անձնական տվյալները ենթարկվում են անվտանգ ջնջման, անանունացման կամ անդառնալի ոչնչացման՝ այնպես, որ բացառվի տվյալների հետագա նույնականացումը կամ վերականգնումը: Այն դեպքերում, երբ տվյալների անմիջական ջնջումը տեխնիկական կամ կարգավորող սահմանափակումների պատճառով հնարավոր չէ, տվյալները պահվում են անվտանգ արխիվացված ձևով, իսկ դրանց հասանելիությունը սահմանափակվում է մինչև վերջնական հեռացումը հնարավոր լինելը:

8.5. Ընկերությունը պահպանում է ներքին տվյալների պահպանման գրաֆիկ, ինչպես նաև իրականացնում է պարբերական վերանայումներ՝ ապահովելու, որ պահված տեղեկատվությունը շարունակի մնալ ճշգրիտ, անհրաժեշտ և օրինականորեն պահպանված: Պահպանման գրաֆիկը հանդիսանում է Ընկերության տվյալների կառավարման և համապատասխանության ընդհանուր շրջանակի բաղադրիչ մաս:

9. Cookie-ներ և վերլուծություն

9.1. Ընկերության պաշտոնական կայքն ու հեռախոսի հավելվածը օգտագործում են cookie-ներ, ծրագրային ապահովման հավաքածուներ և այլ համարժեք հետևման գործիքներ՝ ապահովելու հարթակների անվտանգ աշխատանքը, բարելավելու ֆունկցիոնալությունը և բարձրացնելու օգտատիրոջ փորձը:

9.2. Cookie-ները փոքր տվյալային ֆայլեր են, որոնք տեղադրվում են օգտատիրոջ սարքի կամ բրաուզերի վրա՝ Ընկերության թվային հարթակներին մուտք գործելու պահին: Դրանք հնարավորություն են տալիս ապահովել կայքի հիմնական ֆունկցիոնալությունը, սեսիայի կառավարումը և անհատականացված ծառայությունների մատուցումը, ինչպես նաև ապահովել արտադրողականության վերլուծությունն ու անվտանգության վերահսկումը:

9.3. Ընկերությունը cookie-ներն ու համարժեք տեխնոլոգիաները դասակարգում է հետևյալ կերպ.

- Խիստ անհրաժեշտ Cookie-ներ. Անհրաժեշտ են կայքի կամ հեռախոսի հավելվածի անվտանգ և պատշաճ աշխատանքի համար, ներառյալ՝ նույնականացումը, սեսիայի կառավարումը և գործարքների իրականացումը: Այս cookie-ները հնարավոր չէ անջատել համաձայնության գործիքների միջոցով:
- Նախասիրությունների Cookie-ներ. Օգտագործվում են օգտատիրոջ կարգավորումները հիշելու համար, օրինակ՝ լեզվի ընտրությունը, ցուցադրման նախապատվությունները և մուտքի տարբերակի ընտրությունը՝ ապահովելու ավելի անհատականացված փորձ:
- Վերլուծական և արտադրողականության Cookie-ներ. Հավաքում են ամփոփիչ և անանուն վիճակագրական տվյալներ կայքի օգտագործման և համակարգի աշխատանքային ցուցանիշների վերաբերյալ՝ օգնելու Ընկերությանը բարելավել ծառայությունները և հայտնաբերել տեխնիկական խնդիրները:
- Մարքեթինգային կամ երրորդ կողմի Cookie-ներ. Օգտագործվում են համապատասխան բովանդակություն կամ գովազդային հաղորդագրություններ ցուցադրելու, ինչպես նաև մարքեթինգային արշավների արդյունավետությունը չափելու համար: Սրանք ակտիվացվում են միայն տվյալների սուբյեկտի նախնական համաձայնությամբ:

9.4. Ոչ էական cookie-ների (ներառյալ նախասիրությունների, վերլուծական և մարքեթինգային cookie-ներ) օգտագործումը թույլատրելի է միայն այն դեպքում, երբ օգտատերը տրամադրում է իր հստակ համաձայնությունը՝ GDPR-ի և Հայաստանի Հանրապետության էլեկտրոնային հաղորդակցությունների ու տվյալների պաշտպանության կիրառելի օրենքների համաձայն: Օգտատերերը կարող են ցանկացած պահին հետ կանչել կամ փոփոխել իրենց cookie-ների նախապատվությունները:

9.5. Օգտատերերը կարող են կառավարել կամ անջատել cookie-ները իրենց վեբ-բրաուզերի կամ շարժական սարքի կարգավորումների միջոցով: Սակայն որոշ cookie-ների անջատումը կարող է ազդել կայքի կամ հավելվածի որոշ ֆունկցիաների հասանելիության կամ աշխատանքային արդյունավետության վրա:

9.6. Ընկերությունը կարող է կիրառել վերլուծական գործիքներ, ծրագրային ապահովման հավաքածուներ և երրորդ կողմի ծառայություններ մատուցողներ՝ հավաքելու կայքի կամ հավելվածի աշխատանքի, այցելուների վարքագծի և ծառայությունների օգտագործման միտումների վերաբերյալ ոչ-անձնական տվյալներ: Այդ տվյալները մշակվում են ամփոփիչ կամ անանունացված ձևով և չեն կարող օգտագործվել օգտատերերին անհատապես նույնականացնելու համար:

9.7. Cookie-ների տեսակների, դրանց գործողության տևողության և կառավարման հնարավորությունների վերաբերյալ ավելի մանրամասն տեղեկատվության համար օգտատերերին խորհուրդ է տրվում ծանոթանալ Ընկերության Cookie-ների մասին ծանուցմանը, որը հասանելի է պաշտոնական կայքում:

10. Սույն Քաղաքականության թարմացումներ

10.1. Ընկերությունը պարբերաբար կվերանայի և, անհրաժեշտության դեպքում, կթարմացնի սույն Գաղտնիության քաղաքականությունը՝ ապահովելու համար դրա շարունակական համապատասխանությունը կիրառելի օրենքներին, կարգավորող պահանջներին և Ընկերության ներքին կառավարման ստանդարտներին:

10.2. Թարմացումները կարող են իրականացվել հետևյալ պատճառներով.

- տվյալների պաշտպանության կամ ֆինանսական ոլորտի օրենսդրության փոփոխություններ, ներառյալ Հայաստանի Հանրապետության «Անձնական տվյալների պաշտպանության մասին» օրենքի կամ GDPR-ի փոփոխությունները,
- Հայաստանի Հանրապետության Կենտրոնական բանկի (ՀՀ ԿԲ) կամ այլ իրավասու մարմինների կողմից տրված կարգավորող ուղեցույցների թարմացումներ,
- Ընկերության ներքին գործընթացների, տեխնոլոգիաների կամ ծառայությունների փոփոխություններ, որոնք անդրադառնում են անձնական տվյալների մշակման վրա,
- տվյալների պաշտպանության և թափանցիկության մեխանիզմների ուժեղացման անհրաժեշտություն:

10.3. Սույն Գաղտնիության քաղաքականության ամենաթարմ և ուժի մեջ գտնվող տարբերակը միշտ հասանելի կլինի Ընկերության պաշտոնական կայքում և հեռախոսի հավելվածում: Եթե Դուք շարունակեք օգտվել Ընկերության կայքից, հավելվածից նշված փոփոխություններն ուժի մեջ մտնելուց հետո, ապա կհամարվի, որ Դուք ընդունել եք վերանայված Քաղաքականությամբ սահմանված պայմանները:

10.4. Այն դեպքերում, երբ կատարվում են էական կամ զգալի փոփոխություններ, որոնք կարող են ազդել Հաճախորդների իրավունքների կամ նրանց անձնական տվյալների մշակման ձևերի վրա, Ընկերությունը նախապես կտեղեկացնի Հաճախորդներին՝ էլեկտրոնային հաղորդագրությունների, հավելվածում տեղադրվող ծանուցումների կամ այլ համապատասխան միջոցների միջոցով՝ նախքան փոփոխությունների ուժի մեջ մտնելը:

10.5. Ընկերությունը իրականացնում է տարբերակների վերահսկում և պահպանում է բոլոր փոփոխությունների ներքին հաշվառում՝ ներառյալ յուրաքանչյուր փոփոխված տարբերակի հաստատման ամսաթիվը և այն հաստատած պատասխանատու մարմինը:

11. Կոնտակտային տեղեկատվություն

Տվյալների վերահսկող.
«ԼԵՆԴՄԱՐԿ ԿԱՊԻՏԱԼ» ՓԲԸ
Գրանցված հասցե՝ ՀՀ, քաղաք Երևան, Վազգեն Սարգսյան 10, տարածք 118, 0010
Հեռախոս՝ +374 (60) 277-274
Էլ. հասցե՝ info@landmarkcapital.am
Կայք՝ www.landmarkcapital.am

Տեղեկատվական անվտանգության պատասխանատու / Անձնական տվյալների պաշտպանության պատասխանատու.
Էլ. հասցե՝ information_security@landmarkcapital.am
Հասցե՝ ՀՀ, քաղաք Երևան, Վազգեն Սարգսյան 10, տարածք 118, 0010

Հսկողություն իրականացնող մարմին (ՀՀ).
Անձնական տվյալների պաշտպանության գործակալություն, ՀՀ Արդարադատության նախարարություն
Կայք՝ www.mojustice.am