Жобаны Еуропалық Одақ қаржыландырады

ҰХДБИ

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА

ҮЕҰ-ДА ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ: СЫНАҚТАР МЕН ШЕШІМДЕР

POLICY BRIEF

Бұл жарияланымды Еуропалық Одақ қаржыландырды. Оның мазмұнына тек IWPR жауапты және ол міндетті түрде Еуропалық Одақтың көзқарасын білдірмейді.

2025

Мазмұны

АВТОР ТУРАЛЫ

Құралай Қарақұлова
Заңгер, құқық магистрі.
АҚШ-тың WLP ұйымы сертификаттаған адам құқықтары және әйелдердің құқықтары жөніндегі жаһандық тренер.
Гендерлік теңдік мәселелері бойынша сарапшы.
БҰҰ Даму бағдарламасының Қазақстандағы құқықтық сарапшысы.
Алматы қаласындағы Еуразиялық заңгерлер палатасының мүшесі.

«ЕРКІНДІК ҚАНАТЫ» ҚОҒАМДЫҚ ҚОРЫ ТУРАЛЫ

«Еркіндік қанаты» қоғамдық қоры 2015 жылдың 6 наурызында құрылған.

Қор ұйымдастырушылары мен еріктілерінің белсенді азаматтық ұстанымын қалыптастыру кезінде алынған тәжірибе мен құндылықтарды жинақтаған ашық түрдегі адам құқықтары жөніндегі ұйым.

Қор жұмысының негізгі бағыттары қоғамдық қорғау және құқықтар мен бостандықтарды ілгерілету, білім беру бағдарламалары, зерттеулер жүргізу, оның ішінде мониторинг арқылы жүргізу, сондай-ақ заң шығару қызметіне қатысу болып табылады.

IWPR ТУРАЛЫ

IWPR (Соғыс пен бейбітшілікті баяндау институты) қақтығыс, дағдарыс немесе өтпелі кезеңдегі елдерде жергілікті халықтың дауысын күшейтіп, оң өзгерістерге жол ашады.

Жеккөрушілік тіл мен үгіт-насихат белең алып, журналистер мен азаматтық белсенділер шабуылға ұшыраған кезде, IWPR сенімді ақпарат таратып, қоғам үшін маңызды қоғамдық пікірталастарды қолдайды. Жаңа жалған ақпарат түрлері әлеуметтік араздықты күшейтіп, цифрлық қауіпсіздікке қатер төндіріп, журналистерге шабуылдарды жиілетіп жатқан қазіргі заманда IWPR-дың жергілікті дауыстарды қолдау миссиясы бұрынғыдан да маңызды бола түсті. IWPR-дың негізгі қызметі – журналистер мен азаматтық қоғам өкілдерінің қауымдастықты ақпараттандыруына, ағартуына және жұмылдыруына мүмкіндік беру арқылы сенімді, бейтарап ақпарат ағынын күшейту. IWPR қоғамның өз шешімін өзі табуына көмектеседі, есептілік, сөз бостандығы және адам құқықтары үшін репортаж жасау мен адвокаттық қызмет жүргізу қабілетін арттыру арқылы жергілікті әлеуетті нығайтады.

ЕУРОПАЛЫҚ ОДАҚ ТУРАЛЫ

Еуропалық Одақ – Еуропаның 27 елінен тұратын экономикалық және саяси одақ. Ол – адамның қадір-қасиетін құрметтеу, бостандық, демократия, теңдік, заң үстемдігі және адам құқықтары, соның ішінде азшылық өкілдерінің құқықтарын құрметтеу құндылықтарына негізделген. Қоғам, қоршаған орта және экономиканың тұрақты дамуына жәрдемдесу үшін әркімнің пайдасына орай жаһандық деңгейде әрекет етеді.

КІРІСПЕ

Бүгінде қазіргі заманғы әлемді толықтай цифрлық әлем деп атауға болады. Цифрлық технологиялардың енгізілуі ақпаратты пайдалану арқылы жүзеге асады.

Интернет арқылы берілетін ақпарат көлемі жылдам өсіп келеді. Онлайн-сервистерге тіркелу, әлеуметтік желілер мен мобильді қосымшаларды пайдалану – осының барлығы адамның жеке деректерін енгізумен қатар жүреді.

Алайда, көп адам өздері туралы ақпаратты жариялай отырып, саналы немесе бейсаналы түрде өздерінің жеке деректерін өзгелерге ұсынып жатқанын түсіне бермейді.

Адам туралы ақпарат – бұл өте нәзік жеке дерек, ол алаяқтық, қауіп-қатер, ұрлық және дерек иесіне теріс әсер ету сияқты жағдайларға осал келеді.

Сонымен бірге, жеке ақпарат пен жеке деректер адам құқықтары мен бостандықтарын, әсіресе **жеке өмірге қол сұқпау, жеке құпия мен адамның қадір-қасиетін сақтау** құқықтарын қамтамасыз етумен тікелей байланысты екенін атап өту қажет.

Бұл құқық ең алғаш рет **Адам құқықтарының жалпыға бірдей декларациясының** 12-бабында бекітілген:

«Ешкімнің жеке және отбасылық өміріне, баспанасына, хат алмасуына ерікті түрде араласуға, абыройы мен беделіне қол сұғуға жол берілмейді. Әр адам мұндай араласудан немесе қол сұғудан заңмен қорғалуға құқылы»[1]

Кейін бұл құқық **Азаматтық және саяси құқықтар туралы халықаралық пактінің** 17-бабында нақты айқындалды:

«Ешкімнің жеке және отбасылық өміріне, баспанасына, хат алмасуына заңсыз немесе негізсіз араласуға, ар-намысы мен беделіне заңсыз қол сұғуға жол берілмейді».[2]

Жеке деректер – адамның жеке өмірінің бір бөлігі. Оларды заңсыз жинау мен тарату **адам құқықтарының бұзылуына** алып келуі мүмкін.

1 Всеобщая декларация прав человека, Принята резолюцией 217А (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года

2 Международный пакт о гражданских и политических правах, Принят резолюцией 2200 А (XX1) Генеральной Ассамблеи от 16 декабря 1966 года

Сондықтан бүгінгі таңда жеке деректерді қорғау мәселесі тек халықаралық емес, сонымен қатар ұлттық деңгейде де өзекті күн тәртібіне айналып отыр.

Қазақстан да бұл салада қорғалған емес, сондықтан заңнамалық деңгейде жеке деректер мен оларды қорғау саласындағы мемлекеттік саясаттың негізгі бағыттарын әзірлеп жатыр.

Қазақстандағы жеке деректерді қорғаудың негізгі аспектілері мыналар:

1. Жеке деректерді қорғау бойынша нақты құқықтық кепілдіктер орнату;
2. Жеке дерек субъектілерінің құқықтарын қамтамасыз ету;
3. Деректерді қорғауға арналған ақпараттық және техникалық шешімдер енгізу, сондай-ақ киберқауіпсіздікті дамыту;
4. Жеке деректер туралы заңнаманы бұзған адамдарды жауапкершілікке тарту шараларын қабылдау.

Мемлекеттер, ұйымдар және тұтас қоғам цифрлық технологиялар мен жеке деректерді жинау, өңдеу тетіктері азаматтардың негізгі бостандықтарын бұзбауын қамтамасыз етуге жауапты.

ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУҒА ҚАТЫСТЫ ХАЛЫҚАРАЛЫҚ СТАНДАРТТАР

Жеке деректерді қорғауды халықаралық деңгейде реттеу – жаһандану мен деректер көлемінің өсуі жағдайында маңызды аспект.

Әр түрлі мемлекеттер өздерінің ережелері мен талаптарын белгілегенімен, бүгінгі таңда жеке өмірді қорғауға біртұтас көзқарасты қамтамасыз ететін **халықаралық құжаттар мен қағидаттар** қалыптасқан.

Осындай негізгі халықаралық құжаттардың бірі – **2016 жылғы 27 сәуірде Еуропалық Парламент пен Еуропалық Одақ Кеңесі қабылдаған №2016/679 Регламент**:

«Жеке тұлғаларды жеке деректерін өңдеу кезінде қорғау және мұндай деректердің еркін айналымы туралы» *(GDPR – General Data Protection Regulation)*.

Бұл регламент Еуропалық Одақта қабылданған және 2018 жылғы 25 мамырдан бастап күшіне енген негізгі халықаралық стандарт болып саналады.

Аталған Регламенттің мақсаты – жеке тұлғалардың жеке деректерін өңдеуге қатысты құқықтарын қорғау, деректердің еркін айналымының қағидаларын белгілеу, сондай-ақ жеке тұлғалардың негізгі құқықтары мен бостандықтарын, атап айтқанда, жеке деректерді қорғау құқығын қамтамасыз ету.

Маңызды ерекшелігі – бұл Регламент ЕО аумағындағы жеке деректерді өңдеуге қатысты біріздендірілген ережелерді қамтиды.

Сонымен қатар, Регламент жеке деректерді өңдеудің әмбебап қағидаттарын бекітеді:

5-бап. Жеке деректерді өңдеу қағидаттары

a. Заңдылық, әділет және ашықтық – деректер заңды, адал және дерек субъектісі үшін түсінікті формада өңделуі тиіс;

b. Нақты, айқын және заңды мақсаттар үшін жиналуы тиіс, әрі бұл мақсаттарға сәйкес келмейтін түрде қайта өңделмеуі керек;

c. Деректердің минимизациясы – деректер мақсатқа сай, жеткілікті көлемде және тек қажетті ақпаратпен шектелуі тиіс;

d. Дәлдік – деректер нақты әрі қажет болған жағдайда жаңартылып отыруы тиіс. Қате немесе ескірген деректерді жою немесе түзету бойынша барлық орынды шаралар қабылдануы керек;

e. Сақтау мерзімінің шектеулігі – деректер өңдеу мақсаттарына жету үшін қажет уақыттан артық сақталмауы тиіс;

f. Тұтастық пен құпиялық – деректер тиісті техникалық және ұйымдастырушылық шаралар арқылы рұқсат етілмеген немесе заңсыз өңдеуден, сондай-ақ кездейсоқ жоғалу, жойылу немесе бүлінуден қорғалуы тиіс.

Бұл қағидаттар экстерриториалдық реттеуге ие, бұл дегеніміз – жеке тұлғалардың жеке деректерін жинайтын, өңдейтін және сақтайтын барлық мемлекеттік органдар, ұйымдар мен компаниялар Еуроодақтың Бас регламентінде бекітілген қағидаттарға сай болуы тиіс.
Аталған регламенттің негізгі ерекшелігі – онда **«жеке деректер»** ұғымының өте кең түрде анықталуы.

4-бап. Анықтамалар

«Жеке деректер» – бұл сәйкестендірілген немесе сәйкестендірілуі мүмкін жекетұлғаға(»дерек субъектісі») қатысты кез келген ақпарат; сәйкестендірілуі мүмкін жеке тұлға – бұл тікелей немесе жанама түрде, атап айтқанда, аты, тегі, сәйкестендіру нөмірі, орналасқан жері туралы мәліметтер, онлайн-идентификатор немесе осы тұлғаға тән бір немесе бірнеше физикалық, физиологиялық, генетикалық, рухани, экономикалық, мәдени не әлеуметтік белгілер арқылы анықталуы мүмкін адам.

Сонымен қатар, Регламент деректерді пайдалануға және өңдеуге келісім алуды міндеттейді, деректерді жою құқығын, сондай-ақ ұйымдарда жеке деректерді қорғау жөніндегі маман тағайындау міндетін қарастырады.

Келесі халықаралық құжат – *«Жеке тұлғаларды жеке деректердің автоматтандырылған өңделуі кезінде қорғау туралы конвенция»*, оны 1981 жылғы 28 қаңтарда Еуропа Кеңесіне мүше елдер қабылдаған және бұл тақырыптағы алғашқы құжаттардың бірі.

Конвенцияның мақсаты – әр тараптың аумағында кез келген адамның азаматтығына немесе тұрғылықты жеріне қарамастан, оның жеке деректерінің автоматтандырылған өңделуімен байланысты жеке өмірге қол сұқпау құқығын және негізгі құқықтары мен бостандықтарын құрметтеуді қамтамасыз ету (»деректерді қорғау»).[3]

Сондай-ақ, жеке деректерді қорғауға қатысты осындай құжаттар Азия-Тынық мұхиты аймағында, Канадада, Бразилияда және Африканың кей елдерінде қабылданғанын атап өту қажет.

Аталған құжаттардың барлығы құпиялықтың ерікті қағидаттарын қолдайды және құқықтар мен бостандықтарды қорғау мен бизнесті дамыту арасындағы тепе-теңдікке бағытталған.

Біріккен Ұлттар Ұйымы (БҰҰ) жеке деректерді қорғаудың маңызын мойындайды және жеке ақпараттың құпиялығы мен қауіпсіздігін қамтамасыз етуге бағытталған ұсыныстар мен қағидаттар жиынтығын әзірлеген.

Алғашқы құжаттардың бірі – 2013 жылғы 18 желтоқсанда қабылданған БҰҰ Бас Ассамблеясының 68/167 қарары:

«Цифрлық дәуірдегі жеке өмірге қол сұқпау құқығы»

Аталған қарардың мемлекеттерге жолдаған негізгі үндеуі – жеке өмірге қол сұқпау құқығын құрметтеу және қорғау, соның ішінде цифрлық коммуникация контексінде де, сондай-ақ дерек субъектілерінің құқықтарын сақтау, құқық бұзушылықтардың алдын алу және ұлттық заңнаманы халықаралық адам құқықтары саласындағы міндеттемелерге сәйкестендіру.

3 «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» принятый членами Совета Европы 28 января 1981 году.

РЕЗОЛЮЦИЯЛАР ЖӘНЕ БҰҰ-НЫҢ ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ МӘСЕЛЕЛЕРІН РЕТТЕУ БОЙЫНША САЯСАТЫ

— 2014 жылғы 18 желтоқсандағы БҰҰ Бас Ассамблеясының 69/166 қарары

— Цифрлық дәуірдегі жеке өмірге қол сұқпау құқығы

— БҰҰ Босқындар ісі жөніндегі Жоғарғы Комиссары басқармасының құзыретіне жататын тұлғалардың жеке деректерін қорғау саясаты, 2015 жыл

— 2018 жылғы 11 қазанда БҰҰ Басқару жөніндегі Жоғарғы деңгейдегі комитетінің 36-сессиясында қабылданған Жеке деректер мен құпиялықты қорғау қағидаттары

— 2021 жылғы 7 қазандағы Адам құқықтары жөніндегі кеңестің 48/4 қарары

— Цифрлық дәуірдегі жеке өмірге қол сұқпау құқығы

— БҰҰ Босқындар ісі жөніндегі Жоғарғы Комиссары басқармасының жеке деректер мен құпиялыққа қатысты жалпы саясаты (GDPP), 2022 жыл

Сонымен қатар, БҰҰ 2015 жылдың наурызында жеке өмірге қол сұқпау құқығы мәселелері жөніндегі Арнайы баяндаушы институтын құрды.

Арнайы баяндаушының мандаты оған мына әрекеттерді жүзеге асыруға өкілеттік береді:

- цифрлық хабарламаларды ұстап қалу және жеке деректерді жинау саласындағы мемлекеттік саясат пен заңдарды шолу;
- негізсіз құпиялықты бұзатын әрекеттерді анықтау;
- ғаламдық бақылауды заң үстемдігі қағидатына сай қамтамасыз етудің озық әдістерін әзірлеуде үкіметтерге көмек көрсету;
- адам құқықтарын сақтау бойынша жеке сектордың міндеттемелерін нақтылау;
- ұлттық рәсімдер мен заңнаманы адам құқықтары саласындағы халықаралық міндеттемелерге сәйкестендіруге жәрдемдесу.

Мемлекеттік органдар, коммерциялық ұйымдар және азаматтық қоғам ұйымдары серіктестер мен азаматтардың көз алдында ашық, қауіпсіз және заңды болу үшін осы халықаралық стандарттарды ұстануы тиіс.

ҚАЗАҚСТАНДАҒЫ ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУДЫҢ ҚҰҚЫҚТЫҚ РЕТТЕЛУІ

Қазақстан Республикасы Конституциясының 18-бабына сәйкес:

«Әркімнің жеке өміріне, жеке және отбасылық құпиясына қол сұғылмауына, арнамысы мен қадір-қасиетінің қорғалуына құқығы бар».[4]

Аталған конституциялық норма Қазақстанда мемлекеттік құпиялармен қатар жеке адамның жеке өміріне қатысты ақпараттың да ең жоғары деңгейде қорғалатынын айқындайды.

(Қазақстан Республикасы Азаматтық процестік кодексінің 10-бабына түсіндірме)

«Жеке өмір – бұл адамның тек өзіне ғана қымбат өмірлік кеңістігі, сондықтан қоғам мен мемлекеттің осы салаға тұлғаның өз келісімінсіз араласуына жол берілмейді.

Жеке құпия – жеке өмірдің бір бөлігі ретінде, адамның өзі құпияда сақтауға ниетті мәліметтерінің болуы. Оған денсаулыққа қатысты мәліметтер, интим өмірдің егжей-тегжейлері және т.б. жатады.

Отбасылық құпия – бұл жақын туыстар, яғни отбасы мүшелері бөтен адамдардан жасыратын мәліметтер. Оларға асырап алу құпиясы және басқа да отбасылық қатынастар жатады.

Адам үшін жеке өмірінің маңызын ескере отырып, заң шығарушы оны қол сұғылмаушы деп таниды және кез келген заңсыз араласудан қорғайды.

Жеке деректер адамның жеке өміріне қатысты мәліметтерді қамтитын болғандықтан, жеке деректерді өңдеу және қорғау барысында жеке өмірге қол сұғылмау, жеке және отбасылық құпия құқығын қамтамасыз ету қажет.

Кейін бұл конституциялық норма арнайы заң қабылдау арқылы реттелді. Осылайша, 2013 жылғы 21 мамырда Қазақстан Республикасының **«Жеке деректер және оларды қорғау туралы» Заңы** (бұдан әрі – Заң) қабылданды.

Заңның 2-бабына сәйкес, осы *Заңның мақсаты – жеке деректерді жинау және өңдеу кезінде адам мен азаматтың құқықтары мен бостандықтарын қорғауды қамтамасыз ету.*[5]

4 Конституция Республики Казахстан, принята на республиканском референдуме 30 августа 1995 года
5 Закон Республики Казахстан «О персональных данных и их защите» принят 21 мая 2013 года № 94—V

Заңның маңызды аспектілерінің бірі – жеке деректерді қорғау қағидаттарының бекітілуі.

Заңның 5-бабына сәйкес, жеке деректерді жинау, өңдеу және қорғау келесі қағидаттарға сай жүзеге асырылады:

1. адамның және азаматтың конституциялық құқықтары мен бостандықтарын сақтау;
2. заңдылық;
3. шектеулі қолжетімділіктегі жеке деректердің құпиялығы;
4. дерек субъектілері, иелері және операторлары құқықтарының теңдігі;
5. тұлғаның, қоғамның және мемлекеттің қауіпсіздігін қамтамасыз ету.

Жеке деректер субъектісі – бұл жеке деректерге тікелей қатысы бар, яғни деректер иесі болып табылатын **жеке тұлға ғана** екенін ерекше атап өткен жөн.

Заңда берілген анықтамаға сәйкес, **жеке деректер** ***– бұл белгілі бір немесе осы деректер негізінде айқындалатын дерек субъектісіне қатысты электрон, қағаз және (немесе) өзге материалдық тасымалдағышта тіркелген мәліметтер.***

Яғни, жеке деректер – бұл қандай да бір түрде дерек субъектісіне қатысы бар кез келген ақпарат, оған адамның тұлғасын тікелей немесе жанама түрде анықтауға мүмкіндік беретін белгілер кіреді.

Тәжірибеде жеке деректерге тегі, аты, әкесінің аты, туған күні, азаматтығы, білімі, отбасылық жағдайы, тұрғылықты мекенжайы және дерек субъектісіне қатысты басқа да мәліметтер жатады.

Сонымен қатар, жеке деректер қолжетімділігіне байланысты екіге бөлінеді:

Жалпыға қолжетімді жеке деректер – бұл Қазақстан Республикасының заңдарына сәйкес құпиялықты сақтау талаптары қолданылмайтын және дерек субъектісінің келісімімен ашық қолжетімді болатын мәліметтер.

Шектеулі қолжетімділіктегі жеке деректер – бұл Қазақстан Республикасының заңнамасымен қолжетімділігі шектелген мәліметтер.

3-тармаққа сәйкес, *жеке деректердің иесі және (немесе) операторы, сондай-ақ үшінші тұлға тарапынан жеке деректерді қорғау шараларын іске асыру қағидаларында* жеке деректердің қауіпсіздігіне төнетін қатерлер деп оларды жинау және өңдеу кезінде жеке деректерге санкцияланбаған, соның ішінде кездейсоқ қол жеткізу мүмкіндігін тудыратын шарттар мен факторлардың жиынтығы түсініледі. Мұндай қол жеткізудің салдары ретінде жеке деректерді жою, өзгерту, бұғаттау, көшіру, үшінші тұлғаларға санкцияланбаған түрде беру,

санкцияланбаған түрде тарату, сондай-ақ өзге де заңсыз әрекеттер орын алуы мүмкін.

Заңның 8-бабына сәйкес, жеке деректерді жинауға және өңдеуге келісім келесі мәліметтерді қамтуы тиіс:

«Жеке деректер және оларды қорғау туралы» Заңның 8-бабы, 4-тармағы

1. оператордың атауы (тегі, аты, әкесінің аты (егер жеке басын куәландыратын құжатта көрсетілсе), бизнес-сәйкестендіру нөмірі (немесе жеке сәйкестендіру нөмірі);
2. дерек субъектісінің тегі, аты, әкесінің аты (егер құжатта көрсетілген болса);
3. жеке деректерді жинауға және өңдеуге келісім қолданылатын мерзім немесе кезең;
4. оператордың жеке деректерді үшінші тұлғаларға беру мүмкіндігі туралы немесе мұндай мүмкіндік жоқтығы жөніндегі мәліметтер;
5. деректерді өңдеу барысында жеке деректердің шекарадан тыс берілуі мүмкіндігі туралы мәліметтер;
6. жеке деректердің жалпыға қолжетімді көздерде таратылуы жөніндегі мәліметтер;
7. дерек субъектісіне қатысты жиналатын деректер тізбесі;
8. иесі және (немесе) операторы айқындайтын өзге мәліметтер.

Атап өтетін жайт – 8-тармақшада көрсетілген «иесі және (немесе) оператор айқындайтын өзге мәліметтер». Бұл норма диспозитив сипатқа ие, яғни деректер иесіне нақты белгісіз қосымша мәліметтерді жинауға мүмкіндік береді. Бұл жеке деректер иесіне қатысты манипуляциялар жүргізу үшін түрлі ақпараттарды жинау қаупін туындатады.

Сонымен қатар, «Жеке деректер және оларды қорғау туралы» Заңның 14-бабында мынадай норма бекітілген: *«Жеке деректерді пайдалану олардың иесі, операторы және үшінші тұлға тарапынан тек бұрын мәлімделген жинау мақсаттарына сәйкес жүзеге асырылуы тиіс».*

Бұл дегеніміз, дерек субъектісіне қатысты мәліметтерді жинау көлемі (саны) тек алдын ала нақты көрсетілген мақсаттарға негізделуі тиіс, ал егер мақсат көрсетілмеген жағдайда деректерді жинау заңсыз деп танылады.

Жеке деректерді жинау мен өңдеуді жүзеге асырудың негізгі талаптарының бірі – олардың қорғалуын қамтамасыз ету.

Заңның 1-бабының 11-тармағына, ***«Жеке деректерді қорғау» – бұл осы Заңмен белгіленген мақсаттарда жүзеге асырылатын құқықтық, ұйымдастырушылық және техникалық*** *сипаттағы кешенді шаралар жиынтығы.*

Бұл норма жеке деректермен жұмыс істеу барысында тиісті қорғаныс шараларын қолдану міндетін жүктейді.

Осы мақсатта Заң жеке деректерді жинау, өңдеу және қорғауға байланысты қызметтің құқықтық негіздерін белгілейді. Оған мыналар кіреді:

- ✓ Жеке деректерді қорғау
- ✓ Жеке деректерді жинау
- ✓ Жеке деректерді жинақтау
- ✓ Жеке деректерді сақтау
- ✓ Жеке деректерді өңдеу
- ✓ Жеке деректерді өзгерту
- ✓ Жеке деректерді толықтыру
- ✓ Жеке деректерді пайдалану
- ✓ Жеке деректерді тарату
- ✓ Жеке деректерді тұлғаландырудан ажырату
- ✓ Жеке деректерді бұғаттау
- ✓ Жеке деректерді жою

Заңда жеке деректерді қорғау саласындағы жұмыстарға қандай да бір деңгейде жауапты субъектілердің құқықтары мен міндеттері бекітілген.

Мұндай субъектілерге мыналар жатады:

1. **Жеке тұлға**, яғни жеке деректерге тікелей қатысы бар адам;

2. **Деректер базасының иесі** – жеке деректерді қамтитын базаны иелену, пайдалану және билік ету құқығын іске асыратын мемлекеттік орган, жеке және (немесе) заңды тұлға;

3. **Деректер базасының операторы** – жеке деректерді жинау, өңдеу және қорғауды жүзеге асыратын мемлекеттік орган, жеке және (немесе) заңды тұлға;

4. **Үшінші тұлға** – дерек субъектісі, иесі және (немесе) операторы емес, бірақ жеке деректерді жинау, өңдеу және қорғау бойынша солармен (онымен) байланысты қатынаста немесе жағдайларда әрекет ететін тұлға.

Осы жағдайдағы қоғамдық ұйымдар – бұл жеке деректерді жинау, өңдеу және қорғауды жүзеге асыратын деректер базасының операторлары.

Заңда жеке деректер саласындағы мемлекеттік реттеуді іске асыратын мемлекеттік органдардың құзыреттері белгіленген, сондай-ақ уәкілетті орган айқындалған.

Аталған салада уәкілетті мемлекеттік орган – **Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі (Ақпараттық қауіпсіздік комитеті)**.

27–1-бап. Уәкілетті органның құзыреті

1. жеке деректер және оларды қорғау саласындағы мемлекеттік саясатты қалыптастырады және іске асырады;

1–1) жеке деректер және оларды қорғау туралы Қазақстан Республикасының заңнамасының сақталуына мемлекеттік бақылауды жүзеге асырады;

2. иесі және (немесе) операторы, сондай-ақ үшінші тұлға жүзеге асыратын жеке деректерді қорғау шараларының тәртібін әзірлейді;

2–1) иесі және (немесе) операторы орындайтын міндеттерді жүзеге асыру үшін қажетті және жеткілікті жеке деректер тізбесін айқындау қағидаларын әзірлейді;

2–2) қажетті және жеткілікті жеке деректер тізбесін айқындау тәртібін әзірлейді;

2–3) жеке деректерді қорғау шараларын жүзеге асыру тәртібін айқындайды;

3. дерек субъектісі немесе оның заңды өкілі берген жеке деректер мазмұнының және оларды өңдеу тәсілдерінің өңдеу мақсаттарына сәйкестігі туралы өтініштерді қарайды және шешім қабылдайды;

4. жеке деректер және оларды қорғау туралы ҚР заңнамасын бұзған адамдарды жауаптылыққа тарту шараларын қабылдайды;

5. иесі және (немесе) оператордан, сондай-ақ үшінші тұлғадан жалған немесе заңсыз жолмен алынған жеке деректерді нақтылауды, бұғаттауды немесе жоюды талап етеді;

6. дерек субъектілерінің құқықтарын қорғауды жетілдіруге бағытталған шараларды жүзеге асырады;

6–1) жеке деректер және оларды қорғау мәселелері бойынша кеңесші орган құрады, сондай-ақ оның құрылу және жұмыс істеу тәртібін белгілейді;

6–2) электрондық үкіметтің ақпараттық-коммуникациялық инфрақұрылымының операторына жеке деректердің қауіпсіздігіне нұқсан келтіретін, дерек субъектілерінің құқықтары мен заңды мүдделерінің бұзылу қаупін тудыратын бұзушылықтар туралы ақпарат жібереді;

7. жеке деректерді жинау, өңдеу қағидаларын бекітеді;

7–1) шектеулі қолжетімділігі бар жеке деректерді қамтитын электрон ақпараттық ресурстарда сақтау, өңдеу және тарату үдерістерінің қорғалуын тексеру қағидаларын ҚР Ұлттық қауіпсіздік комитетімен келісу арқылы бекітеді;

7–2) жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервистің жұмыс істеу қағидаларын бекітеді;

7–3) жеке деректерді беру және (немесе) оларға қол жеткізу жүзеге асырылатын жағдайда, мемлекеттік органдар мен (немесе) мемлекеттік заңды тұлғалардың ақпараттандыру объектілерімен мемлекеттік емес ақпараттандыру объектілерінің интеграциясын келіседі;

7–4) жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервистің интеграция қағидаларын бекітеді;

8. осы Заңмен, басқа да Қазақстан Республикасының заңдарымен, Қазақстан Республикасы Президентінің және Үкіметінің актілерімен белгіленген өзге де өкілеттіктерді жүзеге асырады.

Назар аударғымыз келетін маңызды норма – бұл «Жеке деректер және оларды қорғау туралы» Қазақстан Республикасы Заңының 27–2-бабы, ол жеке деректер және оларды қорғау туралы Қазақстан Республикасы заңнамасының сақталуына мемлекеттік бақылау жүргізуді көздейді және Кәсіпкерлік кодекске сәйкес жоспардан тыс тексеру нысанында жүзеге асырылады.

Аталған нормаға сәйкес, мемлекеттік уәкілетті орган, соның ішінде коммерциялық емес ұйымдарды да қамти отырып, «Жеке деректер және оларды қорғау туралы» Заңның сақталуын бақылауға құқылы.

Анықтама үшін: статистикалық деректер

2024 жылдың басынан бүгінгі күнге дейін жеке деректер және оларды қорғау саласындағы Қазақстан Республикасы заңнамасының талаптарын бұзу фактілері бойынша 11 жоспардан тыс тексеру жүргізілді, сондай-ақ 23 әкімшілік іс қозғалып, қаралды. Нәтижесінде, Қазақстан Республикасы Әкімшілік құқық бұзушылық туралы кодексінің 79 және 641-баптарының түрлі тармақтары бойынша 4 жеке тұлға мен 25 заңды және лауазымды тұлғалар әкімшілік жауапкершілікке тартылды, жалпы сомасы 4 910 360 теңге көлемінде айыппұл салынды.

Дереккөз: Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитеті

Алайда, уәкілетті орган мұндай деректерді өз сайтында жарияламайтындықтан, әкімшілік жауапкершілікке тарту динамикасының қалай өзгеріп жатқанын нақты айту мүмкін емес.

Соған қарамастан, біз интернеттегі ашық дереккөздерден белгілі бір динамиканы бақылауға мүмкіндік аламыз. Мысалы, finprom.kz сайтының мәліметінше, биыл қаңтар–шілде айларында Қазақстанда жеке деректер және оларды қорғау туралы заңнаманы бұзудың 65 әкімшілік құқық бұзушылық тіркелген, бұл 2023 жылдың сәйкес кезеңімен салыстырғанда 75,7 пайызға көп. Бұл ретте биыл 61 іс қаралған, ал өткен жылы бар болғаны 23 іс қаралған. Әкімшілік жауапкершілікке тарту туралы қаулы 61 тұлғаға қатысты шығарылған – бұл өткен жылдың осы кезеңімен салыстырғанда 2,9 есе көп. Осы саладағы заңнаманы бұзғаны үшін жалпы сомасы 10,1 млн теңге айыппұл салынса, оның 8,1 млн теңгесі өндірілген. Тағы бір ашық дереккөз – Liter.kz хабарлағандай, 2024 жылы жеке деректерді қорғау саласында 60 жоспардан тыс тексеру және әкімшілік іс жүргізу өткізілген, олардың жалпы сомасы 12 млн 153 мың 455 теңгені құрады. Бұл 2023 жылмен салыстырғанда айтарлықтай жоғары, сол жылы 38 тексеру тіркелген болатын.[6]

Сондай-ақ бұл дереккөз Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі Ақпараттық қауіпсіздік комитетінің төрағасы Руслан Әбдіхалықовтың мына мәліметтерін келтіреді: *«Ақпараттық қауіпсіздікті қамтамасыз ету саласында жыл ішінде 210 жоспардан тыс тексеру және іс жүргізу жүргізілді, олардың жалпы сомасы 7 млн 817 мың 810 теңгені құрады. Электрон құжат және ЭЦҚ саласында 304 мың 519 теңге сомасына 10 әкімшілік іс қаралды».*[7]

6 Источник: https://kapital.kz/tehnology/128514/v—rk—rastet—chislo—pravonarusheniy—svyazannykh—s—zashchitoy—personal—nykh—dannykh.html

7 https://liter.kz/v–kazakhstane–proveli–proverki–na–12–mln–tenge–v–sfere–zashchity–personalnykh–dannykh–1742455826/

Осылайша, жеке деректер туралы заңнаманы бұзғаны үшін әкімшілік істер санының өскенін атап өткен жөн. Мұндай үрдіс жеке деректердің қауіпсіздігін қамтамасыз ету бойынша жұмысты күшейту, сондай-ақ тек азаматтардың ғана емес, сонымен қатар заңды тұлғалардың өкілдерінің де цифрлық сауатын арттыру бойынша шаралар қабылдау қажеттігін көрсетеді.

Айта кету керек, қазіргі таңда жеке деректер саласы мемлекеттің қатаң бақылауында. Мәселен, Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2022 жылғы 29 сәуірдегі №144/НҚ бұйрығына сәйкес Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервистің жұмыс істеу қағидалары бекітілген.

Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервис *(бұдан әрі – ЖБМС)* азаматтың келісімін алғаннан кейін жеке деректерге қол жеткізуді қамтамасыз етуге арналған. Бұл келісім азаматтың жеке деректеріне қол жеткізуге сұраныс жіберетін 1414 нөмірінен SMS-хабарлама немесе субъектінің өзге де жолмен берген келісімі арқылы іске асырылады.

Заңға сәйкес, егер нысандарда жеке деректер болса, мемлекеттік органдардың ақпараттандыру нысандарымен өзара іс-қимыл жасағанда ЖБМС міндетті.

Бүгінгі күні ЖБМС сервисімен 81 ақпараттық жүйе интеграцияланған: олардың ішінде 35-і – мемлекеттік ақпараттық жүйелер, 9-ы – квазимемлекеттік сектордың ақпараттық жүйелері, 37-сі – жеке ақпараттық жүйелер.

ЖБМС сервисі азаматтарға мемлекеттік деректер базаларында сақталған өздерінің жеке деректерін пайдалануды бақылауға мүмкіндік береді – бұл рұқсат беру немесе оған қолжетімділіктен бас тарту арқылы жүзеге асырылады.

Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервистің жұмыс істеуі мен интеграциясын регламенттейтін нормативтік құқықтық актілер:

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2022 жылғы 29 сәуірдегі № 144/НҚ бұйрығы «Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервистің жұмыс істеу қағидаларын бекіту туралы» (Қазақстан Республикасы Әділет министрлігінде 2022 жылғы 7 мамырда тіркелді № 27963);

Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 2022 жылғы 8 шілдедегі № 236/НҚ бұйрығы «Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервиспен интеграциялау қағидаларын бекіту туралы» (Қазақстан Республикасы Әділет министрлігінде 2022 жылғы 13 шілдеде тіркелді № 28786).

Мемлекет жеке деректерді қорғау туралы заңнаманың сақталуына жіті назар аудару жұмысын жалғастыруда.

Мұның дәлелі – 2023 жылғы 28 наурызда «Цифрлық трансформация, ақпараттық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасы 2023–2029 жылдарға арналған» құжатының бекітілуі (Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысымен бекітілген).

Тұжырымдама аясында 10-нысаналы индикатор «Жеке деректерге қол жеткізуді бақылау сервисіне қосылған мемлекеттік ақпараттық жүйелердің үлесі» шеңберінде 2 іс-шара көзделген, бірінші іс-шараны іске асыру мерзімі 2025 жылғы желтоқсанға жоспарланған, ал екінші іс-шара жыл сайынғы негізде іске асырылады.

Бірінші іс-шара шеңберінде жеке сипаттағы деректерді автоматтандырылған өңдеуге қатысты жеке тұлғаларды қорғау туралы Конвенцияға (Конвенция 1981 жылы Еуропа Кеңесімен қабылданған, «Конвенция 108» деген атпен белгілі) қосылу көзделген.

Бұл – тұлғалардың өздерінің жеке деректерін қорғау құқығына арналған алғашқы халықаралық шарт.

Аталған Конвенция Қазақстан азаматтарының жеке деректерін қорғау саласында құқықтарын бұзған шет мемлекеттердің операторларының әрекеттерін тергеуге мүмкіндік береді.

Екінші іс-шара шеңберінде жеке деректерге қол жеткізуді бақылау жүйесімен интеграциялануы тиіс мемлекеттік ақпараттық жүйелердің жыл сайынғы мониторингі көзделген.

Осыған байланысты мемлекет Конвенция мен GDPR нормаларын имплементациялау үшін қажетті барлық рәсімдер мен заңнамалық жұмысты кешенді түрде талдау бойынша тиісті шаралар қабылдап жатқанын атап өту қажет. «Жеке деректер және оларды қорғау туралы» Заңның 29-бабына сәйкес жеке деректер туралы заңнаманы бұзғаны үшін жауапкершілік белгіленген.

Жеке деректер және оларды қорғау, электрон құжат және электрон цифрлық қолтаңба туралы заңнама талаптарын бұзғаны үшін әкімшілік жауапкершілікке тарту өкілеттігі Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетіне жүктелген.

Атап айтқанда, Ақпараттық қауіпсіздік комитеті көрсетілген салалар бойынша Қазақстан Республикасының ӘҚБтК-нің 79, 640 және 641-баптарында көзделген әкімшілік құқық бұзушылық істерді қарайды.

Жоғарыда әкімшілік жауапкершілікке тарту бойынша статистика келтірілген.

ҚР ӘҚБтК 2014 жылғы 5 шілде

79-бап. Жеке деректер және оларды қорғау туралы Қазақстан Республикасының заңнамасын бұзу

1. Жеке деректерді заңсыз жинау және (немесе) өңдеу, егер бұл әрекеттерде қылмыстық жазаланатын әрекет белгілері болмаса,

2. жеке тұлғаларға – отыз, лауазымды адамдарға, жеке нотариустарға, жеке сот орындаушыларына, адвокаттарға, заң кеңесшілеріне, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – алпыс айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.

3. Сол бір әрекеттер, егер олар заңда белгіленген қылмыстық жауаптылыққа әкеп соқпаса, жеке деректердің иесі, операторы немесе үшінші тұлға өзінің қызмет бабын пайдалана отырып жасаған жағдайда жеке тұлғаларға – жүз, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – екі жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.

4. Жеке деректердің иесі, операторы немесе үшінші тұлға тарапынан жеке деректерді қорғау жөніндегі шаралардың сақталмауы, егер бұл әрекетте қылмыстық жазаланатын әрекет белгілері болмаса, жеке тұлғаларға – жүз елу, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – үш жүз айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.

5. Осы баптың үшінші бөлігінде көзделген әрекет, ол жеке деректердің жоғалуына, заңсыз жиналуына және (немесе) өңделуіне әкеп соқса және бұл әрекеттер заңда белгіленген қылмыстық жауаптылыққа әкеп соқпаса, жеке тұлғаларға – екі жүз, лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – жеті жүз елу

6. айлық есептік көрсеткіш мөлшерінде айыппұл салуға әкеп соғады.

Жеке деректер субъектілерінің құқықтарын қорғау мақсатында Қазақстан Республикасының заңдарында көзделген тәртіппен *жеке деректерді жинау, өңдеу және қорғау кезінде субъектінің, иесінің және (немесе) операторының, сондай-ақ үшінші тұлғаның әрекеттері (әрекетсіздігі) даулануы мүмкін екені туралы* 30-бап белгіленген.

«Жеке деректер және оларды қорғау туралы» Заң қабылданғаннан кейін Қазақстан Республикасында жеке деректерді қорғау бойынша арнайы заңнамалық негіздерді қалыптастыру басталды.

Төменде жеке деректерді қорғау қызметін реттейтін кейбір кодекстер, заңдар мен нормативтік құқықтық актілердің тізімі келтірілген:

№	Нормативтік құқықтық актілердің атауы	
1.	Еңбек кодексі	2015 жылғы 23 қарашадағы № 414-V
2.	Әлеуметтік кодекс	2023 жылғы 20 сәуірдегі № 224-VII ҚРЗ
3.	«Халық денсаулығы және денсаулық сақтау жүйесі туралы» кодекс	2020 жылғы 7 шілдедегі № 360-VI
4.	Кәсіпкерлік кодекс	2015 жылғы 29 қазандағы № 375-V
5.	«Прокуратура туралы» Конституциялық заң	2022 жылғы 5 қарашадағы № 155-VII
6.	«Онлайн-платформалар және онлайн-жарнама туралы» заң	2023 жылғы 10 шілдедегі № 18-VIII ҚРЗ
7.	«Мемлекеттік статистика туралы» заң	2010 жылғы 19 наурыздағы № 257-IV
8.	«Ақпараттандыру туралы» заң	2015 жылғы 24 қарашадағы № 418-V
9.	«Қаржы нарығы мен қаржы ұйымдарын мемлекеттік реттеу, бақылау және қадағалау туралы» заң	2003 жылғы 4 шілдедегі № 474-II
10.	Жеке деректерді жинау, өңдеу қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 21 қазандағы № 395/НҚ бұйрығы

11.	Иесінің және (немесе) оператордың, сондай-ақ үшінші тұлғаның жеке деректерді қорғау шараларын іске асыру қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2023 жылғы 12 маусымдағы № 179/НҚ бұйрығы
12.	Иесінің және (немесе) оператордың өз міндеттерін орындауы үшін қажет және жеткілікті жеке деректер тізбесін айқындау қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2023 жылғы 21 маусымдағы № 199/НҚ бұйрығы
13.	Электрон ақпараттық ресурстарда қамтылған шектеулі қолжетімді жеке деректерді сақтау, өңдеу және тарату процестерінің қорғалуын қамтамасыз етуге тексеру жүргізу қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2021 жылғы 30 сәуірдегі № 156/НҚ бұйрығы
14.	Стратегиялық жоспарлау және реформалар агенттігі, Ұлттық статистика бюросы жүзеге асыратын міндеттерді орындау үшін қажет және жеткілікті жеке деректер тізбесі	Стратегиялық жоспарлау және реформалар агенттігі төрағасының 2022 жылғы 24 маусымдағы № 3 бұйрығы
15.	Жеке деректер субъектілеріне жеке деректер қауіпсіздігінің бұзылғаны туралы хабарлау қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 2024 жылғы 9 тамыздағы № 481/НҚ бұйрығы
16.	Жеке деректер және оларды қорғау мәселелері жөніндегі консультатив кеңеске қатысты кей мәселелер туралы	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2022 жылғы 12 сәуірдегі № 118/НҚ бұйрығы

17.	Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервис жұмыс істеу қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2022 жылғы 29 сәуірдегі № 144/НҚ бұйрығы
18.	Иесінің және (немесе) оператордың, сондай-ақ үшінші тұлғалардың жеке деректер және оларды қорғау туралы заңнаманы сақтауын тексеру парағы	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2024 жылғы 19 наурыздағы № 149/НҚ және Премьер-Министрдің орынбасары – Ұлттық экономика министрінің 2024 жылғы 19 наурыздағы № 12 бірлескен бұйрығы
19.	Жеке деректерге қол жеткізуді бақылау бойынша мемлекеттік сервиспен біріктіру қағидалары	Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің м.а. 2022 жылғы 8 шілдедегі № 236/НҚ бұйрығы
20.	Шектеулі қолжетімді жеке деректерді сақтау және беру ақпаратты криптографиялық қорғау құралдарын қолдана отырып жүзеге асырылады, олар үшінші деңгейдегі қауіпсіздік параметрлерінен төмен болмауы тиіс	ҚР СТ РК 1073–2007 «Ақпаратты криптографиялық қорғау құралдары. Жалпы техникалық талаптар» стандарты

Осылайша, деректер қауіпсіздігі саласындағы жаһандық үрдістер мен сын-қатерлерді ескере отырып, Қазақстан халықаралық қағидаттарға сәйкес келетін тиімді қорғаныс жүйесін құруға ұмтылуда.

ҚАЗАҚСТАНДАҒЫ ҚОҒАМДЫҚ ҰЙЫМДАРДА ЖЕКЕ ДЕРЕКТЕРДІ ҚОРҒАУ МӘСЕЛЕЛЕРІ БОЙЫНША «ЕРКІНДІК ҚАНАТЫ» ҚҚ 2025 ЖЫЛҒЫ АҚПАН–НАУРЫЗ АЙЛАРЫНДА ЖҮРГІЗГЕН САУАЛНАМА НӘТИЖЕЛЕРІНІҢ ТАЛДАУЫ

2025 жылғы ақпан мен наурыз аралығында «Еркіндік қанаты» қоғамдық қоры Қазақстандағы қоғамдық ұйымдарда (бұдан әрі – ҮЕҰ) жеке деректерді қорғау мәселелері бойынша сауалнама жүргізді.

Аталған онлайн-сауалнаманың мақсаты – Қазақстандағы үкіметтік емес ұйымдарда жеке деректерді қорғау тәжірибесін зерделеу болды.

Зерттеу жүргізу барысында екі түрлі әдіс қолданылды:

1. онлайн-сауалнама
2. фокус-топтар

Онлайн-сауалнамаға Қазақстанның әртүрлі өңірлерінен 117 үкіметтік емес ұйымның өкілдері қатысты.

Айта кету керек, 2023 жылғы сәуірдегі жағдай бойынша тіркелген ҮЕҰ саны – 23 335 (дереккөз: ҚР Ақпарат және мәдениет министрлігі Ақпарат комитеті).[8]

Сауалнама нәтижелерін талдау үшін уәкілетті мемлекеттік органда мемлекеттік тіркеуден өткен ***111 ұйымның*** жауаптары іріктелді.

Сауалнама 33 сұрақтан тұрады және бірнеше бөлімге бөлінген. Зерттеу мақсатын ашатын өзекті сұрақтардың жауаптары талдауға алынды.

САУАЛНАМА НӘТИЖЕЛЕРІ

1.1 Сауалнаманың бірінші бөлімінде ұйым туралы негізгі әкімшілік-ұйымдастырушылық ақпарат көрсетілді.

Сауалнамаға Қазақстанның 17 өңірінен үкіметтік емес ұйымдар қатысты. Ең көп жауаптар мына өңірлерден түсті: Алматы қаласынан – 27 (23,5 %), Астана қаласынан – 17 (14,8 %), Қостанай облысынан – 8 (7,0 %), Шығыс Қазақстан об-

8 https://www.gov.kz/memleket/entities/inf/activities/142?lang=ru

лысынан – 8 (7,0 %), Павлодар облысынан – 7 (6,1 %) және Түркістан облысынан – 7 (6,1 %).

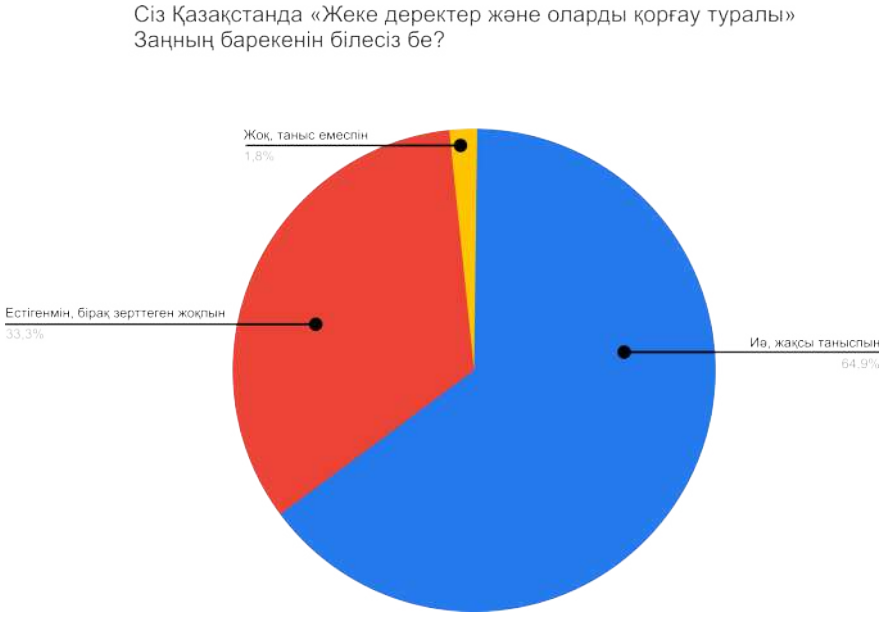
Ұйымдағы қызметкерлер/еріктілер санына келсек, көпшілігі 10 адамнан аз: 5–10 адам аралығында – 38,9 %, 5 адамнан аз – 36,3 %.

2024 жылы ұйым қандай да бір жобаларды жүзеге асырғаны туралы сұраққа жауаптар былай бөлінді: ұйымдардың жартысынан көбі (55,8 %) 1–5 жоба іске асырған, 14,2 % ешқандай жоба жүзеге асырмаған, ал 9,7 % 10-нан астам жоба өткізген.

Сауалнама нәтижелері көрсеткендей, респондент ұйымдардың ең көбі (35,2 %) адам құқықтары саласында жұмыс істейді, одан кейінгі орында білім беру саласы (16,4 %), ал үшінші орында – экология саласы (11,4 %)

2.2. Сауалнаманың екінші бөлімі жеке деректерді қорғау туралы хабардарлық мәселелеріне арналды.

«Сіз Қазақстан Республикасының «Жеке деректер және оларды қорғау туралы» Заңын білесіз бе?» деген сұраққа респонденттердің 64,9 %-ы бұл заңмен жақсы таныс екенін айтты. Ал 33,3 %-ы заң туралы естігенін, бірақ оны оқымағанын көрсетті.



Сонымен қатар, респонденттердің 52,3 %-ы уәкілетті орган ретінде ЦДИАӨМ жанындағы Ақпараттық қауіпсіздік комитетін дұрыс көрсетті.

Алайда, респонденттердің үштен бірі (28,8 %) бұл саланы реттейтін мемлекеттік органды атауға қиналды. Қалған респонденттер дұрыс емес жауаптарды таңдаған немесе мүлде жауап бермеген.

Сондай-ақ, ұйым командасының дербес деректерді қорғау туралы хабардар болу деңгейін бағалау кезінде орташа деңгей көрсетілгенін атап өткен жөн – 45,9 %. Респонденттер әріптестерінің білімін орташа деп санайды, ал тек 14,4 % ғана хабардар болу деңгейін жоғары деп бағалаған.

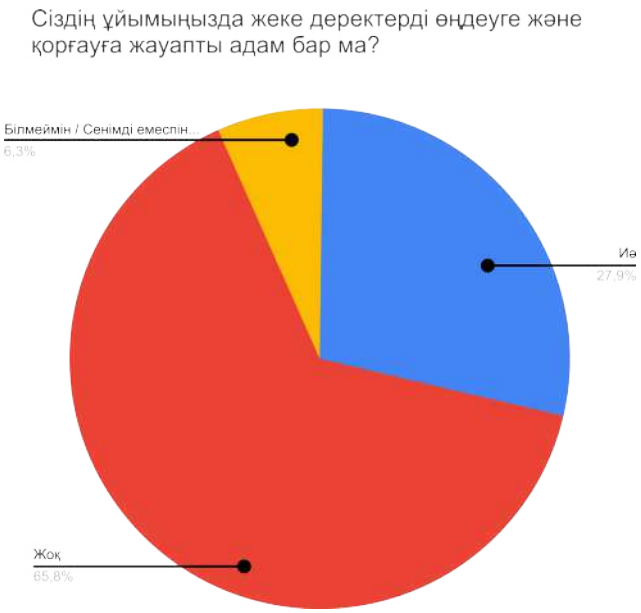
Хабардар болудың төмен деңгейін 19,8 % респондент атап өткен.

3.1. Сауалнаманың үшінші бөлімі ұйымдардағы дербес деректерді басқарудың қазіргі тәжірибесі туралы

Сұрақтардың біріне сәйкес, ұйымның дербес деректерді жинау, өңдеу және сақтау бойынша регламенті/ережесі бар ма дегенге тек 39,6 % ұйым өздерінде ішкі саясат және/немесе деректерді өңдеу регламенттері бар екенін көр-

сеткен. Ал 38,7 % ұйымда мұндай құжаттар мүлде жоқ. Сонымен қатар, 18,9 % ұйым мұндай ішкі құжаттарды әзірлеп жатқанын мәлімдеген.

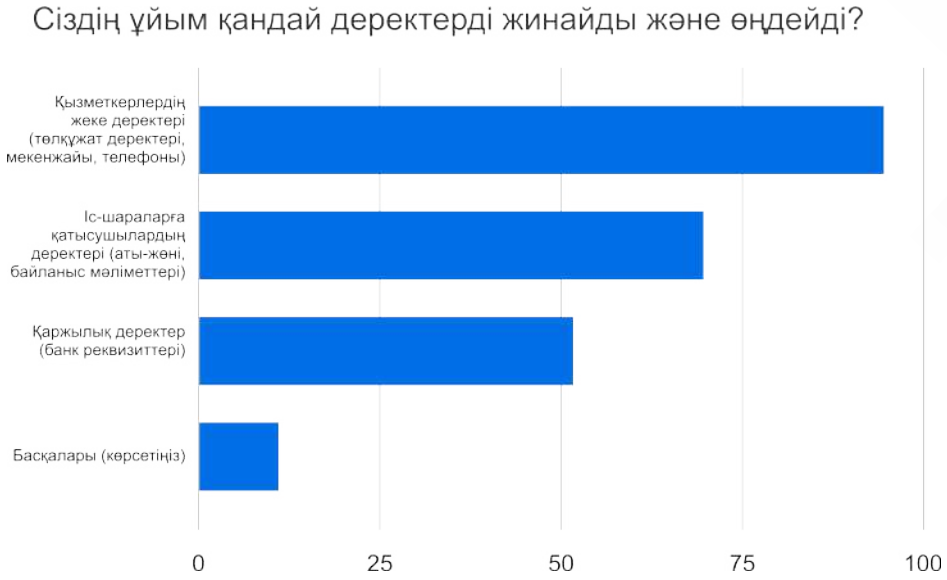
Сонымен бірге, тек 27,9 % респондент өз ұйымында дербес деректерді өңдеу және қорғау үшін жауапты тұлға тағайындалғанын көрсеткен. Өкінішке қарай, 65,8 % респондент мұндай жауапты тұлға тағайындалмағанын айтқан.



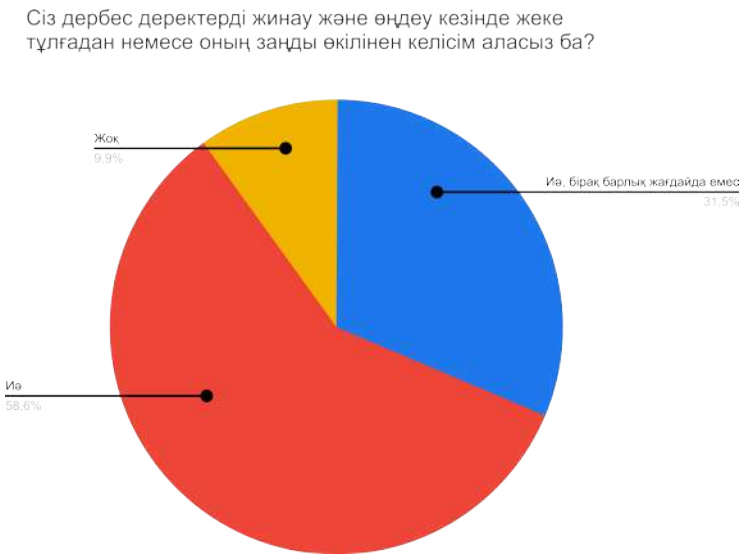
«Ұйым қандай деректерді немесе құжат түрлерін жинайды?» деген сұраққа жауап бергенде көптеген ұйымдардың қызметкерлердің жеке деректерін (төлқұжат деректері, мекенжайы, телефоны) жинайтыны және өңдейтіні анықталды. Бұдан кейін іс-шараларға қатысушылардың деректерін жинау атап өтілді, атап

айтқанда – аты-жөні, байланыс мәліметтері. Үшінші орында – қаржылық деректер (банктік реквизиттер).

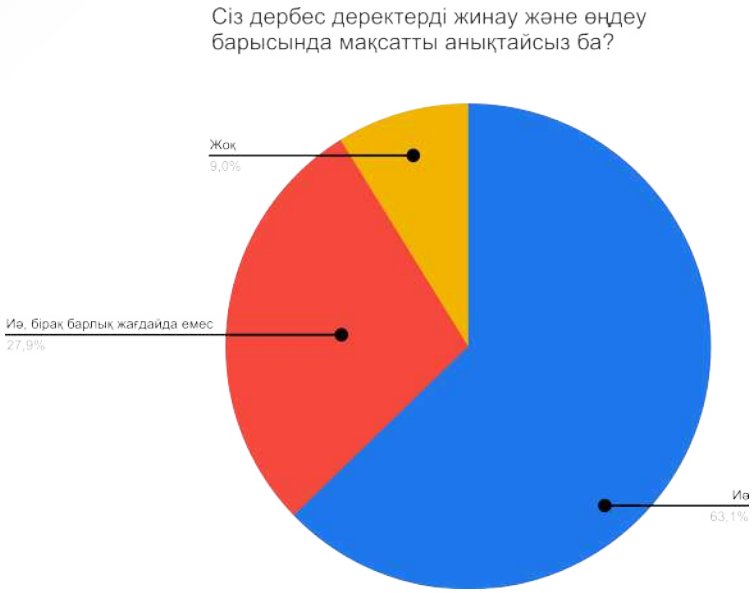
«Басқалары» санатында кей респонденттер медициналық ақпаратты, басқа бенефициарлардың құжаттарын, әлеуметтік бағдарламалар туралы ақпаратты көрсеткен. Алайда, сауалнама барысында кейбір ұйымдар мүлде дербес деректер жинамайтынын да көрсеткен.



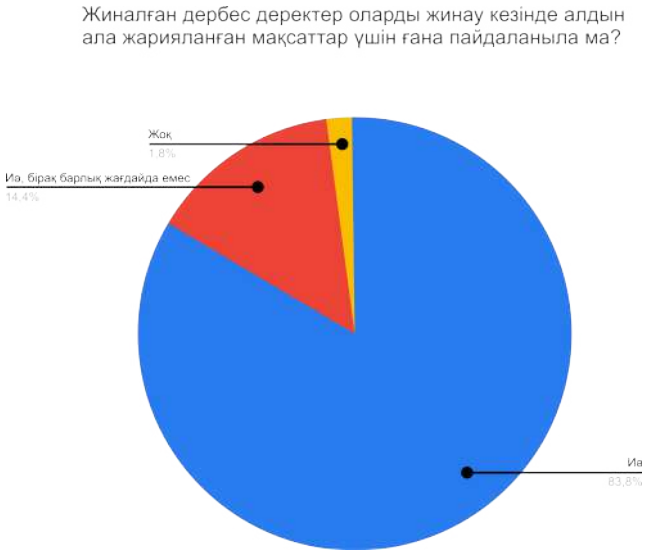
Дербес деректерді жинау және өңдеу кезінде ұйым жеке тұлғадан немесе оның заңды өкілінен келісім ала ма деген сұраққа респонденттердің 58,6 %-ы деректерді өңдеуге келісім алатынын көрсетті, ал 31,5 %-ы мұны барлық жағдайда жасамайтынын айтты. Тек 9,9 % ғана келісім алмайтынын көрсеткен.



Сонымен қатар, дербес деректерді жинау мен өңдеудің мақсаттарын анықтау мәселесінде сауалнама нәтижелері респонденттердің жартысынан астамы (63,1 %) деректерді жинау барысында мақсатты нақты көрсететінін көрсетті. Алайда, 27,9 % респондент бұл мақсатты үнемі нақтылай бермейтінін айтты.



Жиналған дербес деректер бұрын жарияланған мақсаттар үшін ғана пайдаланыла ма деген сұраққа жауаптардың 83,8 %-ы жоғары бағаны көрсетті. Тек 14,4 % жағдайда ғана деректер үнемі емес, бұрын жарияланған мақсаттар үшін пайдаланылады.

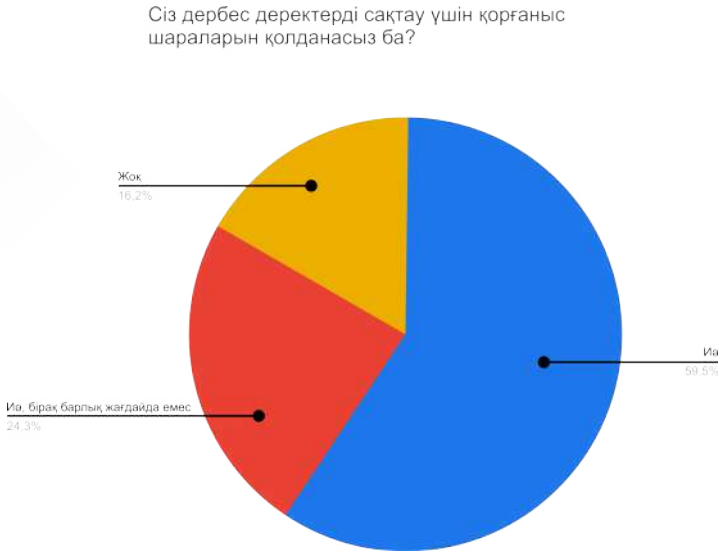


Ұйым дербес деректерді жалпыға қолжетімді және шектеулі қолжетімді деректерге бөле ме деген сұраққа 57,7 % респондент деректерді ажырататынын көрсетті. Ал 28,8 % респондент деректерді ажыратпайтынын айтты. Алайда, 13,5 %

жауап бергендер мұның не екенін білмейтінін атап өткен жөн.

Сауалнама нәтижелері көрсеткендей, дербес деректерді сақтау былай жүзеге асырылады: ұйымдардың көпшілігі деректерді жергілікті базада сақтайды (47,1 %), қағаз түріндегі тасымалдағыштарда сақтайтындар – 32,4 %, ал бұлтты сервистерде сақтайтындар – 18,8 %.

Дербес деректерді сақтау кезінде қорғаныс шаралары қандай деңгейде қолданылып жатыр дегенге жауаптар келесідей бөлінді: 59,5 % респондент деректерді қорғау шараларын (құпиясөз, шифрлау сияқты) қолданатынын айтты, ал ұйымдардың шамамен ширегі (24,3 %) бұл шараларды тұрақты түрде қолданбайды, ал 16,2 % мүлде ешқандай қорғаныс шараларын қолданбайды.



Маңызды атап өтетін жайт, бұл сауалнамада 10 ұйым дербес деректердің ықтимал таралу жағдайлары туралы хабарлады. Аталған оқиғалар қатарына қатқыл дискілер мен компьютердің ұрлануы, «Пегасус» бағдарламасының қолданылуы, дербес деректердің шетелдік интернет-ресурстарда жариялануы, сондай-ақ электрон-поштаның құпия сөзінің таралуы кірді.

4.1 Сауалнаманың төртінші бөлімі ұйымдардың қандай қиындықтар мен қажеттіліктерге тап болатынын, сондай-ақ қоғамдық ұйымдарда дербес деректерді қорғау үшін қандай шаралар қажет екенін анықтауға арналды.

Ұйымдар дербес деректерді қорғау саласында қандай қиындықтарға тап болатыны туралы сұраққа берілген жауаптардың нәтижелері қоғамдық ұйымдардың бұл саладағы негізгі мәселелері мыналар екенін көрсетті:

– Қызметкерлерде білім мен машықтың жетіспеушілігі – 54,9 %

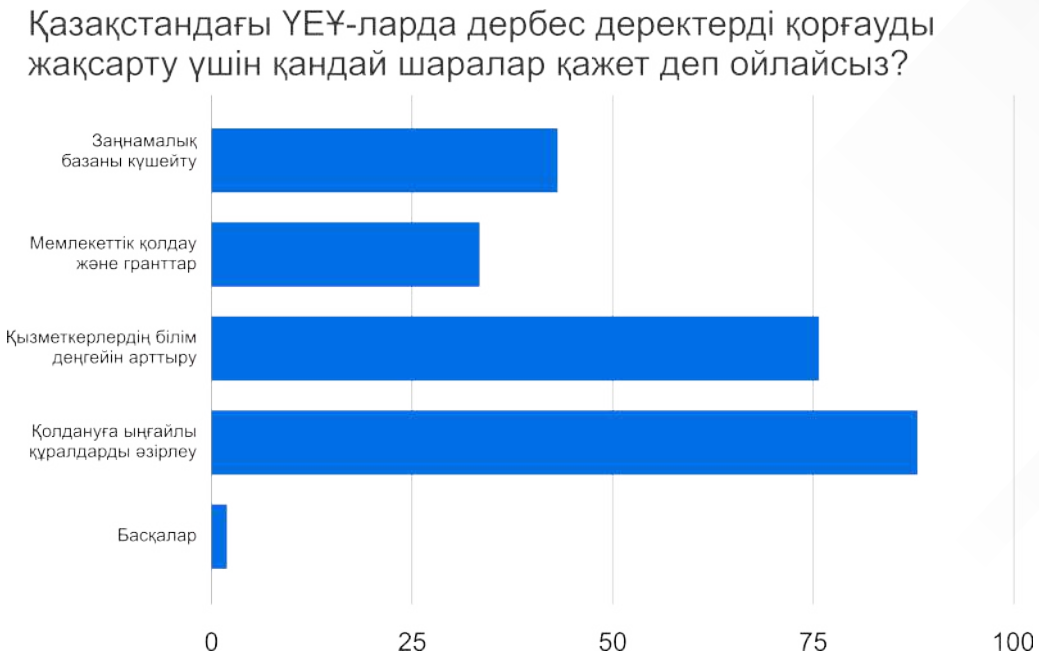
– Қорғау шараларын енгізуге арналған қаржылық ресурстардың шектеулігі – 49,6 %

– Бағдарламалық қамтамасыз ету немесе жабдық сияқты техникалық құралдардың жетіспеушілігі – 46,9 %

– Заңдық немесе техникалық көмекке қол жеткізу мәселелері – 36,3 %

– Заңнамалық талаптарды түсінбеу – 33,6 %

– Қызығушылық танытатын немесе жауапты қызметкерлердің болмауы – 29,2 %



«Қазақстандағы YEҰ-ларда дербес деректерді қорғауды жақсарту үшін қандай шаралар қажет?» деген сұраққа мына ұсыныстар айтылды:

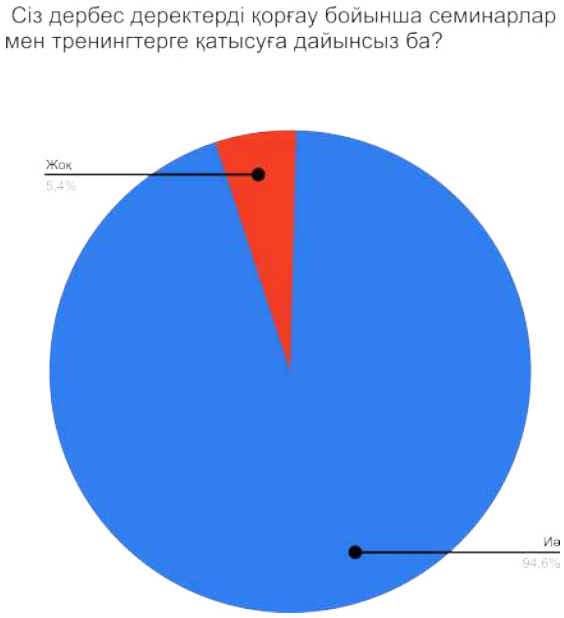
– Респонденттердің көпшілігі дербес деректерді қорғауға арналған қолжетімді құралдар әзірлеуді ұсынды;

– Одан кейінгі орында ұйым қызметкерлерінің білім деңгейін арттыру;

– Заңнамалық базаны күшейту;

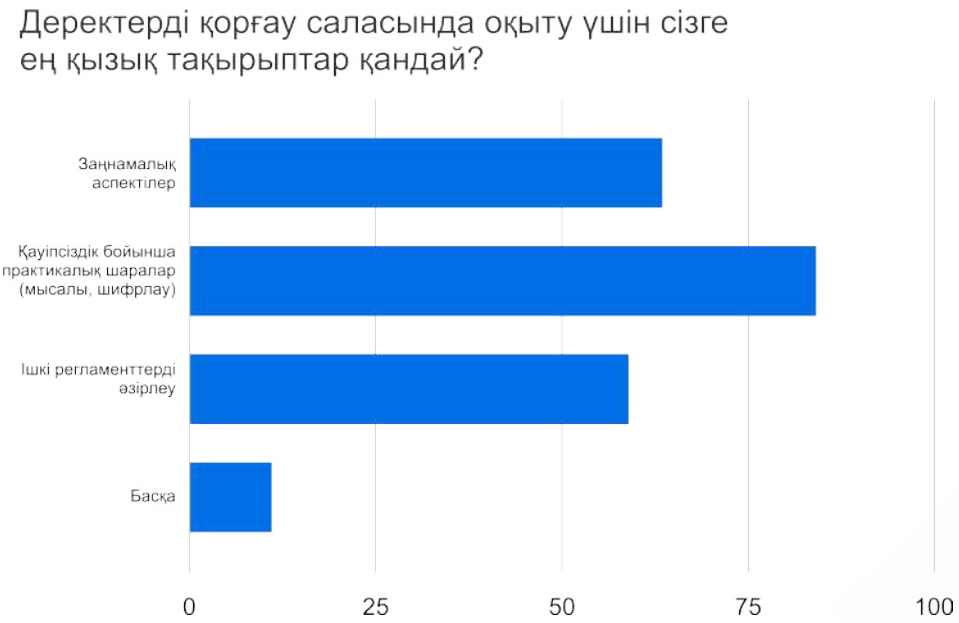
– Мемлекеттік қолдау мен гранттар.

Айта кетерлігі, бұл тақырып бойынша білім алуға деген қажеттілік өте жоғары екені байқалады. «Сіз дербес деректерді қорғау бойынша семинарлар мен тренингтерге қатысуға дайынсыз ба?» деген сұраққа 94,6 % респондент «Иә» деп жауап берген.



Сонымен қатар, жауаптар барысында дербес деректерді қорғау саласындағы оқыту үшін ең қызығушылық тудыратын тақырыптар анықталды:

1. Қауіпсіздік бойынша практикалық шаралар (мысалы, шифрлау)
2. Заңнамалық аспектілер
3. Ішкі регламенттерді әзірлеу



2025 ЖЫЛДЫҢ АҚПАН–НАУРЫЗ АЙЛАРЫНДА «ЕРКІНДІК ҚАНАТЫ» ҚҚ ӨТКІЗГЕН ҚАЗАҚСТАНДАҒЫ ҚОҒАМДЫҚ ҰЙЫМДАРДА ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУ МӘСЕЛЕЛЕРІ БОЙЫНША ФОКУС-ТОП НӘТИЖЕЛЕРІНІҢ ТАЛДАУЫ

Зерттеу аясында сауалнама жүргізумен қатар, 5 фокус-топ өткізілді (оның 2-і Астанада офлайн, ал 3-і онлайн форматта өтті).

Фокус-топтарға Қазақстанның 9 өңірінен 29 қоғамдық ұйымның өкілдері қатысты: Астана, Алматы, Түркістан облысы, Өскемен, Павлодар, Орал, Семей, Атырау және Тараз қаласы.

Фокус-топтардың мақсаты – дербес деректерді өңдеуге байланысты тәжірибе мен қиындықтарды тереңірек зерттеу, сондай-ақ онлайн-сауалнама нәтижелерін нақтылау және тексеру болды.

Талқылаулар барысында сауалнама арқылы алынған негізгі тұжырымдар расталды және нақты қоғамдық ұйымдардың тәжірибесіне сүйене отырып, контекстпен толықтырылды. Сонымен қатар, жұмыс барысында кездескен нақты мысалдар да айтылды.

Сауалнамадағыдай, фокус-топтардың көпшілігін құқық қорғау бағытындағы ұйымдар құраса да, қатысушылар арасында зерттеумен, шығармашылық жобалармен, экологиямен және басқа да салалармен айналысатын ұйымдар болды.

Талдау үшін тақырыптық талдау (thematic analysis) әдісі қолданылды, бұл әртүрлі ұйымдар жұмысының ұқсастықтары мен айырмашылықтарын анықтауға мүмкіндік берді.

ФОКУС-ТОП НӘТИЖЕЛЕРІ

1. Дербес деректермен жұмыс істеу саясаты

Сауалнама мен фокус-топ нәтижелері көрсеткендей, қоғамдық ұйымдардың көпшілігінде дербес деректермен жұмыс істеуге арналған жеке, ресми саясаты немесе регламенті жоқ.

Сонымен қатар, талқылау барысында кей ұйымдардың ішкі құжаттарында мұндай саясаттың жекелеген элементтері бар екені анықталды. Мысалы, кей жағдайларда қызметкерлермен келісімшарт жасасу кезінде дербес деректерді жария етпеу туралы келісімдер жасалады, сондай-ақ деректерді жинау кезінде оларды өңдеуге келісім алынады. Кей ұйымдарда дербес деректермен жұмыс істеу тәртібі ішкі рәсімдердің бір бөлігі ретінде құжаттарда көрсетілген, мысалы, бенефициарлармен жұмыс істеу немесе іс-шараларды ұйымдастыру кезіндегі құжаттарда бекітілген.

Респонденттердің жауаптарынан үзінділер

«Бұрын біз жеке куәліктің көшірмесін құжаттамада сақтау үшін сұрайтынбыз. Заңнама өзгергендіктен, біз бұл әрекетті тоқтаттық. Қазір біз адамдардан жеке куәлік деректерін жазбаша түрде ұсынуды немесе келісімшартқа өздері енгізуін сұраймыз. Яғни, біз енді келісімшарттарға ешқандай куәлік көшірмесін қоспаймыз.» (Алматы)

«Қазақстандағы коммерциялық емес ұйымдардың басым бөлігі өте ықшам [...], кейде бір адамнан тұратын ұйымдар да болады. Орта есеппен алғанда, коммерциялық емес ұйымдардың штаты 3–5 адамнан тұрады. Бұл саясат кімге арналған деген сұрақты түсіну маңызды. Яғни, егер қандай да бір күрделі бизнес-процестер мен еңбек қатынастары шеңберінде коммуникациялар болса, саясат орынды. Ал көп жағдайда коммерциялық емес сектордағы ұйымдар үшін көптеген саясаттардың қажеттілігі міндетті емес болып көрінеді. Мысалы, бізден кадрлармен жұмыс істеу саясатын талап етеді. Егер ол тек директор, есепші мен координатордан тұрса, қандай кадрлық жұмыс болмақ? Мұндай жағдайларда мұның бәрін жеке еңбек шарттарына тіркелген лауазымдық нұсқаулықтармен реттеуге болады ғой.» (Алматы)

«Біз салықтық мақсаттар үшін барлық бастапқы қаржылық құжаттаманы 10 жыл бойы, зейнетақы мақсатында өмір бойы сақтауымыз керек болғандықтан, қызметкерлер штатына қатысты барлық ақпаратты міндетті түрде мұрағаттаймыз. Мұрағаттау белгілі бір ережелер мен талаптарға сәйкес жүргізіледі. Барлығы кеңседе үш құлыптың артында сақталады. Электрон түрде бастапқы құжаттама тек донорларға қаржылық есептің сканерленген көшірмесін жіберу қажет болғанда ғана сақталады. Бұл мәліметтер де мұрағатталады, бұлтты сақтау форматында, бірақ тек донорлардың талап еткен мерзімі бойы сақталады. Бұл 3, 5 немесе 10 жыл болуы мүмкін – бұл стандарт сақтау мерзімдері.» (Өскемен)

Жеке деректермен жұмыс істеу бойынша толыққанды саясаттарды енгізгендердің ішінде екі негізгі топты бөліп көрсетуге болады. Біріншісі – мұндай құжаттарды **донорлардың (негізінен шетелдік) талаптарына сәйкес қабылдаған** ұйымдар. Екіншісі – **оқыту бағдарламаларынан кейін саясатты өздері әзірлеп,** күнделікті тәжірибеде оның маңызын түсіне отырып пайдаланатындар.

Сонымен қатар, екі топтың да өкілдері құжаттағы барлық ережелерді тәжірибеде сақтау өте қиын екенін атап өтеді. Негізгі себептер – уақыт жетпеуі, адами ресурстардың тапшылығы және ұйымдық мүмкіндіктердің шектеулілігі, бұл әсіресе тек жоба іске асыруға бағытталған шағын қоғамдық ұйымдарға тән.

2. Жүйелі көзқарастың болмауы

Алдыңғы бөлімде айтылғандай, қоғамдық ұйымдардың жеке деректермен жұмыс істеу тәжірибесіндегі екінші маңызды ерекшелік – жүйелі көзқарастың болмауы. Бұл, ең алдымен, ресурстардың шектеулілігі және заң талаптарын түсінудегі қиындықтармен байланысты. Деректерді қорғау мақсатында іс жүзінде барлық ұйымдар белгілі бір әрекеттер жасайды. Мысалы, сақтауға арналған қорғалған орындарды пайдаланады (металл сейфтер сияқты), жобалар аяқталғаннан кейін жеке деректерді жояды, екі факторлы аутентификация, күрделі құпиясөздер қолданады, сондай-ақ онлайн-формалар арқылы деректерді жинау кезінде келісім мәтіндерін қосады.

Алайда бұл шаралар жүйелі сипатта емес және жиі біртұтас стратегиясыз немесе үйлестірусіз жүзеге асырылады. Қоғамдық ұйымдардың жұмыс жағдайында бірнеше адам әртүрлі функцияларды қатар атқарады, ал негізгі назар жобаларды жүзеге асыруға бағытталған кезде, деректерді қорғау мәселелері басымдыққа ие болмайды.

Сонымен қатар, «Жеке деректер және оларды қорғау туралы» Заңмен таныс болуына қарамастан, респонденттер құқықтық талаптарды практикада қолданудағы түсініктің жеткіліксіздігін және уәкілетті органдардан түсіндіру жұмысының аздығын атап өтеді. Ұйымдарға олардың қызметінің ерекшеліктері мен нормаларды іс жүзінде іске асыру мүмкіндіктерін ескеретін бейімделген түсіндірмелер, нұсқаулықтар мен мысалдар жетіспейді.

3. Донорлармен жұмыс

«Бізде әр жолы донорға деректерді беру мәселесі туындайды, себебі біз бұл деректердің донорда сақталуына кепілдік бере алмаймыз, мейлі ол шетелдік ұйым, халықаралық немесе мемлекеттік ұйым болсын [...] Талаптар кейде құжаттардың көшірмесіне дейін барады.» (Өскемен)

Фокус-топтар барысында көтерілген маңызды тақырыптардың бірі – донорлармен, әсіресе бенефициарлардың жеке деректерін беру контекстіндегі өзара әрекеттестік болды. Коммерциялық емес ұйымдардың қызметінің ерекшелігі халықаралық және мемлекеттік донорлармен жұмыс істеу және олардың алдындағы міндетті есептілікпен тығыз байланысты.

Кей жағдайларда жобаның іске асырылғанын, көрсетілген қызметтер мен игерілген бюджетті растау үшін донорлар тек жалпыға қолжетімді деректерді (мысалы, аты-жөні) ғана емес, сондай-ақ құжаттардың көшірмелері, диагноз анықтамалары, әлеуметтік мәртебелер туралы ақпарат сияқты сезімтал мәліметтерді де сұратады.

Ұйымдар өз құрылымдарының ішінде деректерді қорғауды қамтамасыз ете алады. Алайда деректер донорға берілгеннен кейін олардың әрі қарайғы пайдаланылуы мен сақталуын бақылау мүмкін болмай қалады.

Бұл мәселе, әсіресе, Азаматтық бастамаларды қолдау орталығы (АБҚО) арқылы реттелетін мемлекеттік гранттармен жұмыс істеу кезінде өткір көрінеді. Респонденттердің айтуынша, гранттық келісімдер мәтінінде жобалар қатысушыларының жеке деректерін (аты-жөні, байланыс деректері және басқа да ақпараттар) беру талабы тікелей көрсетіледі. Бұл коммерциялық емес ұйымдар үшін деректерді беруге қатысты заңды міндет пен оларды қорғау жауапкершілігі арасында қайшылық туғызады.

Сонымен қатар, талқылау барысында жобалар аяқталғаннан бірнеше жыл өткен соң бенефициарларға мемлекеттік органдардың өкілдері хабарласып, олардың жобаларға қатысуы туралы сұрақтар қойған жағдайлар аталып өтті. Бұл деректердің коммерциялық емес ұйымдарға бағынбайтын құрылымдарда ұзақ уақыт сақталатынын көрсетеді.

4. Мемлекеттік органдардың жауапкершілігі

Фокус-топтар барысында коммерциялық емес ұйым өкілдері арасында жеке деректермен жұмыс істеуге байланысты тұрақты алаңдаушылық сезімі байқалды. Бұл тек білім мен ресурстардың жетіспеушілігімен ғана емес, сонымен қатар бенефициарлар тарапынан сенімсіздік және мемлекеттік құрылымдар жағынан ықтимал қауіппен байланысты, оған ішкі жүйелердің бұзылуы немесе тексерулер жатады.

Көптеген ұйымдар бенефициарлар жеке деректерді беруге барған сайын көбірек қорқатынын атап өтеді, бұл жағдай кибералаяқтық оқиғаларының жиілеуіне байланысты. Бұл әсіресе қарт адамдармен жұмыс істейтін жобаларда байқалады.

Сонымен қатар, мемлекеттік органдар ұйымдардың ішкі деректеріне қол жеткізе алады деген қорқыныш бар. Қатысушылар мұндай араласу жағдайлары бұрын болғанын айтты. Мысалы, Тараз қаласынан бір респондент ұйымға қызмет көрсетіп, гонорар алған маманға полиция тарапынан олардың қызметі туралы сұрақтар мен қоңыраулар түскен жағдайды сипаттады. Ұйым тарапынан ешқандай деректер берілмеген, ал мұндай ақпараттың көзі ретінде респондент тек мемлекеттік немесе банктік жүйелер болуы мүмкін деп есептейді.

Респонденттің жауабынан үзінді

«Ұйымнан гонорар алған барлық бенефициарларға үшінші тұлғалардан, полиция қызметкерлерінен, банк қызметкерлерінен, тіпті ҰҚК өкілдерінен қоңыраулар келіп түсті. Бұған дейін айтылғандай, басты қауіп – мемлекет тарапынан. Мен мұны өз жеке тәжірибемнен растай аламын, себебі бұл ақпаратты менен басқа ешкім білмейді. Мен ұйымның есебін өзім жүргіземін, яғни ақпараттың таралуы тек менің салық комитетіне берген есебім арқылы немесе шоттардың жағдайын және сома көлемін көре алатын банк менеджерлері тарапынан болған.» (Тараз)

Бұл жағдай ұйым барлық заң талаптарын сақтағанның өзінде де қорғалмауы мүмкін екенін көрсетеді. Соның нәтижесінде деректерді қорғау мәселесі тек техникалық және құқықтық сала емес, ұйымның қауіпсіздігіне тікелей әсер ететін фактор ретінде қабылданады.

Маңыздысы, заңнамалық негізсіз мемлекеттік органдар ұйым қызметкерлерінің дербес деректерін талап етуге құқылы емес.

Дербес деректерді жинау және өңдеу, жекелеген жағдайларды қоспағанда, тек субъектінің немесе оның заңды өкілінің келісімімен жүзеге асырылады. Сонымен қатар дербес деректерді жинау, өңдеу және пайдалану тек оператор белгілеген мақсаттар шеңберінде жүзеге асырылуы тиіс. Осы мақсатқа жету үшін қажетті дербес деректердің нақты және анық тізімі де оператор тарапынан жасалуы керек.

Субъектінің немесе оның заңды өкілінің келісімінсіз дербес деректерді жинауға және өңдеуге рұқсат берілетін жекелеген жағдайлар «Дербес деректер және оларды қорғау туралы» Заңның 9-бабында көрсетілген.

Аталған респонденттің жауабында сипатталған жағдай осындай ерекшелікке жатуы мүмкін – ол әкімшілік құқық бұзушылық істерін, атқарушылық өндірісті қозғайтын және қарайтын құқық қорғау органдары, соттар және өзге де уәкілетті мемлекеттік органдардың қызметімен байланысты. Алайда бұл істер өндірісте болуы, тергеу жүргізілуі немесе тексеру шеңберінде жүзеге асырылуы тиіс.

5. Дербес деректермен тұрақты жұмыс істеу үшін ұйымдардың қажеттіліктері мен ұсыныстары

Осы зерттеу шеңберінде жүргізілген сауалнамалар мен фокус-топтардың нәтижелері Қазақстандағы қоғамдық ұйымдар тек ресурстық шектеулермен ғана емес, сонымен қатар дербес деректермен жұмыс істеу мәселелерінде жүйелі, түсінікті әрі қолжетімді қолдаудың аздығымен бетпе-бет келетінін көрсетті. Бұл шектеулер ұйымдардың ішкі мүмкіндіктерімен де, құқықтық реттеудің қазіргі деңгейімен де байланысты.

Ұйымдар тарапынан айқын байқалған қажеттіліктердің бірі – заңнама, соның ішінде жаңа қосалқы нормативтік актілер бойынша қолжетімді оқыту, сондай-ақ құқық қолдану саласындағы кеңес беру мен сүйемелдеу.

Қоғамдық ұйым өкілдері заңмен жай танысудың жеткіліксіз екенін атап өтеді – нормаларды тәжірибе тіліне «аудару» қажет: заңгер емес қарапайым адамдарға арналған түсінікті материалдар, көрнекі әдістемелер, нұсқаулықтар мен жадналамалар. Мысалы, үнемі қолжетімді онлайн-курстар, қадамдық әрекеттері бар қысқа бейнедәрістер.

Маңызды ұсыныстардың бірі – автоматтандырылған құралдарды жасау. Мысалы, Telegram-бот, ол келісімдер, саясат үлгілерін жасап беріп, деректерді жою қажеттілігі туралы ескертіп отыра алады.

Көптеген респонденттер қазіргі ресурс тапшылығы – қаржылық та, кадрлық та жағдайда қоғамдық ұйымдарда заңгерлерді немесе арнайы бөлімдерді ұстауға мүмкіндік жоқ екенін айтты. Сондықтан аутсорсинг немесе секторға бейімделген дайын шешімдер туралы идея өзекті болып отыр. Бизнес саласында қолданылатын дайын өнімдер тәжірибесі коммерциялық емес секторға бейімделе алады.

Ұсыныстардың бір бөлігі заңнамалық және институционалдық ортаға қатысты. Фокус-топ қатысушылары мынадай ұсыныстар айтты:

- Әкімшілік айыппұлдарды, әсіресе коммерциялық емес ұйымдарға қатыстыларын жеңілдету керек, репрессив тәсілдерден бас тарту қажет.
- Заңдарды бұзғаны үшін ғана емес, талаптарды сақтағаны үшін де марапаттау маңызды: мысалы, гранттық конкурстарда артықшылықтар беру, тәжірибені мойындау.
- Заңдар нақты, түсінікті әрі әртүрлі түсіндірмелерге жол бермейтін болуы керек. Қазір олар әртүрліше түсіндіріледі, бұл құқықтық белгісіздік тудырады.

- Нормаларды әзірлеу кезінде тек мемлекеттік органдар ғана емес, тәуелсіз сарапшылар мен қоғамдық ұйым өкілдері де қатысуы тиіс.

- Мемлекет үлгі көрсетуі тиіс: мемлекеттік органдардан деректердің жиі таралып кетуі (және оның ресми түрде мойындалуы) заң талаптарына деген сенімді төмендетеді.

- Мемлекет тек бақылаушы емес, қолдаушы тарап болуға тиіс. Қоғамдық ұйымдар мемлекеттің шынайы әрекетін, ашық коммуникация арналары мен орталықтандырылған ресурстарды, сондай-ақ шағымдану тәртібі мен жедел көмек алуға мүмкіндік беретін нақты алгоритмдерді көргісі келеді. Бұған жедел желі, қолжетімді заңгерлік қолдау да кіреді.

ҚОҒАМДЫҚ ҰЙЫМДАРДАҒЫ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУҒА БАЙЛАНЫСТЫ ҚАУІПТЕР МЕН ТӘУЕКЕЛДЕР

Сауалнама мен фокус-топ нәтижелері дербес деректерді қорғау саласындағы бірқатар ортақ мәселелер мен тәуекелдерді анықтады. Көптеген респонденттер дербес деректерді қорғаудың маңызын атап өткенмен, кей қатысушылар «Дербес деректер және оларды қорғау туралы» Заңның мазмұнын толық түсінбейтінін көрсетті.

Зерттеудің негізгі мақсаты – Қазақстандағы қоғамдық ұйымдарда дербес деректердің қорғалу ахуалын кешенді түрде бағалау болғандықтан, сауалнама жалпылама сипатта жүргізілді.

Сонымен қатар, қоғамдық ұйым өкілдерінің басым бөлігі «Дербес деректер және оларды қорғау туралы» Заңмен таныс екенін және бұл салада білім деңгейін арттыруға мүдделі екенін көрсетті.

Сауалнама нәтижелері негізінде дербес деректерді қорғау саласындағы негізгі қауіптер мен тәуекелдер ретінде мыналар ұсынылады:

1. **Технологиялық жаңашылдықтар** – белгісіз шешімдер, мобильді қосымшалар және өзге де технологиялардың жылдам дамуы дербес деректерді өңдеу мен қорғауға жаңа талаптар қояды.

2. **Заңдар мен нормалардың жиі өзгеруі** – нормативтік-құқықтық актілерге енгізілетін өзгерістер мен толықтырулар ішкі саясаттар мен дербес деректерді қорғау рәсімдерін үнемі жаңартуды талап етеді.

3. **Білім мен машықтың жетіспеушілігі** – дербес деректер субъектілері өз деректерін кімге, не үшін және қандай көлемде беретінін түсіне бермейді. Бұл құқықтық талаптарды орындауды қиындатады және ұйымдар тарапынан заң бұзушылықтарға әкеп соғады.

4. **Ресурстардың шектеулілігі** – қоғамдық ұйымдардың дербес деректерді қорғау бойынша заманауи жүйелерді енгізуге, арнайы мамандарды тартуға және қызметкерлерді оқытуға қаржылық мүмкіндіктері жоқ.

5. **Өзіндік бақылаудың болмауы** – дербес деректер субъектілері өз деректерінің кейінгі тағдырын бақылай алмайды, бұл деректерді теріс пайдалану тәуекелдерін арттырады.

6. Құжаттарды кездейсоқ немесе әдейі көшіру, ақпаратты басып шығару арқылы жария ету – бұл әрекеттер де маңызды қауіп тудырады.

Сонымен қатар, келесі тәуекелдер дербес деректер иелеріне де, қоғамдық ұйымдардың өзіне де зиян келтіруі мүмкін:

1. Деректердің сыртқа таралуы – деректермен дұрыс жұмыс істемеу оларды жоғалтуға алып келуі мүмкін. Ақпараттың таралу арналары: алынбалы тасымалдаушылар, электрон-пошта, қағаз құжаттар, компьютерлер мен мобильді құрылғылар.

2. Мәліметтер базасына заңсыз қол жеткізу – бағдарламалық қамтамасыз етудегі осалдықтар және адами фактор.

3. Сыртқы қауіптер – кибершабуылдар, фишинг, зиянды бағдарламалар және т.б.

4. Ішкі қауіптер – қызметкерлер тарапынан кеткен қателіктер, білімнің жетіспеушілігі, заңнаманы білмеу.

5. Бақылаудың болмауы – бағдарламалық жасақтама мен деректерді сақтау/өңдеу жүйелерін жаңартып отырмау оларды осал етеді.

6. Алаяқтық немесе деректерді теріс пайдалану – адамдардың сеніміне кіру арқылы жасалатын қылмыстар.

7. Заңнаманы бұзу – дербес деректерді қорғау талаптарын орындамау айыппұлдарға және ұйым жұмысының тоқтатылуына әкеп соғуы мүмкін.

8. Цифрлық сауаттың төмен деңгейі – халықтың бір бөлігінің деректермен және технологиялармен жұмыс істеу машығы жоқ, бұл деректерді тиімді пайдалану мен қауіпсіздікке кері әсер етеді.

Осы тәуекелдер мен қауіптерге жауап ретінде жүйелі әрі кешенді тәсіл қажет. Бұл – қызметкерлерді оқытудан бастап, ұйым ішіндегі институционалдық жүйені жетілдіру, дербес деректерді басқару саясатын дамыту және барлық мүдделі тараптардың белсенді қатысуын қамтиды.

ҰСЫНЫСТАР

Адам құқықтарын сақтау, жеке деректерді қорғау, сондай-ақ тәуекелдердің, құпиялықты бұзу, жеке деректерді қорғау саласындағы заңнама нормаларын бұзудың алдын алу мақсатында тиісті шаралар қабылдау қажет.

Өткізген сауалнама қоғамдық ұйым өкілдерінің өз ұйымында қандай шаралар, саясаттар мен құжаттарды қабылдау қажеттігі туралы түсінігі төмен екенін көрсетті. Осыған байланысты мынадай **ұсыныстар** беріледі:

1. **Қоғамдық ұйымдарға** мына құжат түрлері түрінде практикалық құралдарды әзірлеу ұсынылады:

1. Жеке деректерді қорғау және өңдеу саясаты. Бұл құжат Заң нормаларына және ұйымның қызметінің ерекшеліктеріне негізделе отырып әзірленуі тиіс.

2. Қызметкерлердің жеке деректері туралы ереже. Құжаттың негізінде Қазақстан Республикасының Еңбек кодексі нормалары ескерілуі тиіс, соның ішінде қызметкердің Ережемен танысу құқығы.

3. Қызметкерлердің жеке істерін жүргізу тәртібі, олардағы жеке деректерді өңдеу, сақтау және беру қағидалары туралы ереже.

4. Құпиялық саясатын әзірлеу және енгізу. Құжат ұйым қандай ақпаратты жинайтынын, ол қалай пайдаланылатынын және оған кімнің қол жеткізе алатынын нақты көрсетуі тиіс.

5. Жеке деректерді өңдеуге келісім беру формасы. Бұл форма «Жеке деректер және оларды қорғау туралы» Заң негізінде дайындалуы тиіс.

6. Қызметкерлерді оқыту бағдарламасын әзірлеу. Жеке деректерді қорғау бойынша үздік тәжірибелер мен ақпараттың таралуының алдын алу тәсілдері туралы хабардарлықты арттыру мақсатында тұрақты түрде тренингтер өткізу.

7. Деректерді шифрлау, қорғау және сақтау бағдарламасын әзірлеу. Бағдарламаны әзірлеу үшін маман тарту қажет.

8. Жұмыс беруші актілері. Деректерді өңдеу жүйелеріндегі осал тұстарды анықтау және оларды уақтылы жою үшін аудиттер мен тексерулерді тұрақты түрде өткізуге байланысты.

9. Жеке деректерді сақтау туралы ереже. Жеке деректерді сақтау мерзімін және оларды жинау мен сақтау мақсаты орындалғаннан кейін жою тәртібін қамту қажет.

10. Жеке деректерді қорғау саласындағы заңнаманы сақтау туралы жұмыс берушінің актілері. Ұлттық және халықаралық заңнаманы зерттеу. Жеке деректердің таралуы немесе заңсыз пайдаланылуымен байланысты тәуекелдерді азайту.

11. Осал тұстарды талдау. Деректерді өңдеу жүйелерінде тұрақты түрде ену сынамаларын (penetration testing) өткізу және осал тұстарды анықтау.

12. Хабардар ету. Жеке деректерді өңдеу және қорғау қағидаттары туралы ақпараттық материалдар (буклеттер, жаднамалар, ішкі таралымдар) әзірлеу.

13. Қолданыстағы тәжірибелерді тұрақты түрде талдау. Бұл заң талаптарын орындауға, клиенттер мен серіктестердің сенімін арттыруға көмектеседі.

14. Жеке деректермен жұмыс істеуге жауапты маманды тағайындау туралы бұйрық.

Сауалнамаға қатысушылардың аз ғана бөлігі жеке деректерді қорғауды мемлекеттік реттеу мәселелері бойынша, атап айтқанда, осы саладағы уәкілетті мемлекеттік органның қандай екенін нақты атай алды.

Сонымен қатар, бейінді Заңда белгілі бір қоғамдық қатынастарды реттеудегі олқылықтар бар екенін ескере отырып, келесі ұсыныстар беріледі:

2. Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігіне:

1. Қоғамдық ұйымдардың қажеттіліктерін ескере отырып, жеке деректерді өңдеуге арналған жалпы стандарттар мен әдістемелік ұсынымдар әзірлеу

2. Жеке деректерді қорғау саласындағы мемлекеттік органдар мен қоғамдық ұйымдар өкілдерінің қатысуымен дөңгелек үстелдер ұйымдастыру және өткізу

3. Қоғамдық ұйымдарға жеке деректерді қорғау мәселелері бойынша құқықтық және кеңестік көмек көрсетуге арналған арнайы бағдарламалар әзірлеу

4. Қоғамдық ұйым өкілдеріне құқықтық нормаларды түсіндіру мақсатында оқыту семинарларын, тренингтер ұйымдастыру және өткізу

5. Жеке деректер субъектілерін олардың деректерімен жасалатын әрекеттер туралы хабардар ету тәртібін реттейтін Ережелер әзірлеу және қабылдау

6. Пайдалану мақсаты аяқталғаннан кейін жеке деректерді жою тәртібін реттейтін Ережелерді әзірлеу және қабылдау. Мұндай нақты рәсімнің болмауы оны өз бетінше жүзеге асыруда түсініксіздіктерге алып келуі мүмкін

7. Жеке деректерді жинауға және өңдеуге келісім беру кезінде сақталуы тиіс өлшемдер тізбесін (мысалы, ерікті, мәжбүрлеудің болмауы, хабардар етілуі және т.б.) әзірлеу және қабылдау. Қолданыстағы Заңда мұндай өлшемдер тізбесі жоқ

7-тармаққа түсініктеме

«Жалпыға қолжетімді дереккөз» ұғымының нақты анықтамасының болмауы жеке деректер субъектісінің құқықтарын бұзуға әкеп соғуы мүмкін.

Мысалы, жалпыға қолжетімді дереккөзде жеке деректер субъектісі жариялауға ниет білдірмеген ақпарат болуы мүмкін. Сонымен қатар, әртүрлі жалпыға қолжетімді дереккөздерден жеке деректерді біріктіру адам туралы бұрмаланған пікір қалыптастырып, оның беделіне немесе өмірінің басқа да қырларына теріс әсер етуі ықтимал. Сондай-ақ, бұрын жалпыға қолжетімді дереккөздерде жарияланған нақты емес немесе ескірген жеке деректерді пайдалану адам туралы қате қорытындыға әкелуі мүмкін, бұл жеке деректер субъектісінің құқықтарының бұзылуына әкеп соғады.

Бұл мәселеге қатысты ақпараттық қауіпсіздік комитетінің өтініш беруші қойған сұрағына жауабы бар: *«Жалпыға қолжетімді ақпаратты қамтитын кез келген онлайн-платформаны немесе өзге дереккөзді, яғни заң талаптарына сәйкес шектелуі мүмкін емес немесе ақпаратты өзі (жеке немесе заңды тұлға) жариялайтын (тарататын) дереккөзді жалпыға қолжетімді деп санауға бола ма?»* деген сұраққа Комитет: **«...әлеуметтік желілерді жалпыға қолжетімді дереккөздерге жатқызуға болады» деп жауап береді.**

Алайда, «Нормативтік құқықтық актілер туралы» Заңның 60-бабына сәйкес, **мұндай түсіндірмелердің міндетті заңдық күші жоқ және ұсымдық сипатқа ие.**

8. «Жалпыға қолжетімді дереккөз» ұғымын заңнама терминологиясына енгізу, өйткені бұл тіркес Заңның 7-бабында қолданылған, алайда нақты анықтамасы жоқ

Жеке деректерді үшінші тұлғалар тарапынан қайта жинау, өңдеу және тарату жағдайларына нақтылау енгізу қажет, өйткені қолданыстағы Заңда қайта жинау кезінде келісім талап етілетіні туралы норма қарастырылмаған (Заңның 7-бабының 3 және 4-тармақтары).

ҚОРЫТЫНДЫ

Бүгінде қызметкерлерді жұмысқа қабылдау кезінде жеке деректерді қорғау, жинау, өңдеу және сақтау аспектілері, шарттар жасасу кезінде жеке деректермен алмасу ерекшеліктері, интернеттегі жеке деректерді қорғау, сондай-ақ оларды сақтау және жою мәселелері ерекше өзектілікке ие.

Сонымен қатар, денсаулық сақтау, білім беру және әлеуметтік көмек сияқты әртүрлі салаларда жұмыс істейтін қоғамдық ұйымдар қатысушылардың, еріктілер мен тұтынушылардың деректерінің құпиялығы мен қауіпсіздігін қамтамасыз ету бойынша ерекше міндеттерге ие.

Алаяқтықтан, жеке деректерді заңсыз пайдаланудан қорғайтын тиімді басқару стратегиясын әзірлеу арқылы ұйым жұмысының тиімділігін арттыратын технологияларды қолдану мен азаматтардың жеке деректерінің құпиялығы мен қауіпсіздігін қорғау арасындағы теңгерімді қамтамасыз етуге болады.

Жеке деректерді қорғауды дұрыс және сауатты басқару деректердің таралуының алдын алуға, мүдделі тараптардың сенімін арттыруға мүмкіндік береді, бұл кез келген ұйымның тұрақты дамуының негізгі аспектісі.

Қоғамдық ұйымдар жеке деректерді қорғауға байланысты қауіп-қатерлер мен тәуекелдерді белсенді түрде ескеріп, оларды азайту үшін стратегиялық тәсілдер әзірлеуі қажет.

Бүгінде жеке деректердің қауіпсіздігін қамтамасыз етудің көптеген құралдары мен әдістері бар, олардың ішінде шифрлау, қол жеткізуді бақылау жүйелерін пайдалану, тұрақты аудиттер және қызметкерлерді оқыту ерекше маңызға ие.

Қауіпсіздік мәселелерінде адами фактор жиі шешуші рөл атқаратынын атап өту маңызды, сондықтан қызметкерлердің тәуекелдер мен қорғау әдістері туралы хабардарлығын арттыру әр қоғамдық ұйым үшін басымдыққа айналуы тиіс.

Ұйымдарда жеке деректердің қауіпсіздігін қамтамасыз ету бойынша мақсаттарға қол жеткізу үшін мына негізгі әрекеттерге назар аудару қажет:

1. Қауіпсіздік саясаты
2. Тәуекелдерді бағалау
3. Қызметкерлерді оқыту
4. Қорғаудың техникалық шаралары
5. Мониторинг және әрекет ету

Сондай-ақ, тек ұлттық заңнаманы ғана емес, сонымен қатар GDPR сияқты деректерді қорғау саласындағы халықаралық стандарттарды сақтау қажеттілігін де ескеру қажет. Бұл құқықтық салдардан аулақ болуға көмектесіп қана қоймай, ұйымның жақсы беделі мен бәсекеге қабілеттілігінің кепіліне айналады.

Қоғамдық ұйымдар жеке деректерді қорғау саласындағы заңнаманы жетілдіру бойынша бастамашы болуы тиіс. Мұндай бастамалар болашақта жеке ақпаратты өңдеуге қауіпсіз орта қалыптастыруға ықпал етеді.

Осылайша, қоғамдық ұйымдарда жеке деректердің қауіпсіздігін арттыруға бағытталған кешенді шараларды енгізу жай ғана қажеттілік емес, тез өзгеретін цифрлық орта жағдайында тұрақтылыққа жету үшін стратегиялық таңдау.

Қоғамдық ұйымдарда жеке деректерді қорғау жай ғана заңдық міндет емес, сонымен бірге олардың әлеуметтік жауапкершілігінің маңызды аспектісі.

Халықтың жеке деректерді қорғау, цифрлық құқықтар туралы хабардарлығын арттыру – қоғамда орнықты экожүйе құрудың алғышарты.

Деректерді қорғау бойынша шаралардың сәтті жүзеге асырылуы тек заңнаманы сақтауға ғана емес, сонымен қатар азаматтық қоғамның дамуына ықпал ететін сенімді және ашық институттар ретінде қоғамдық ұйымдардың қалыптасуына да мүмкіндік береді.

ӘДЕБИЕТТЕР ТІЗІМІ

1. Всеобщая декларация прав человека, Принята резолюцией 217A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года.

2. Международный пакт о гражданских и политических правах, Принят резолюцией 2200 A (XX1) Генеральной Ассамблеи от 16 декабря 1966 года.

3. «Конвенция о защите физических лиц при автоматизированной обработке персональных данных» принятый членами Совета Европы 28 января 1981 году.

4. Конституция Республики Казахстан, принята на республиканском референдуме 30 августа 1995 года.

5. Закон Республики Казахстан «О персональных данных и их защите» принят 21 мая 2013 года № 94-V.

6. https://kapital.kz/tehnology/128514/v-rk-rastet-chislo-pravonarusheniy-svyazannykh-s-zashchitoy-personal-nykh-dannykh.html

7. https://liter.kz/v-kazakhstane-proveli-proverki-na-12-mln-tenge-v-sfere-zashchity-personalnykh-dannykh-1742455826/

8. https://www.gov.kz/memleket/entities/inf/activities/142

Жобаны Еуропалық
Одақ қаржыландырады

ҰХДБИ

ERKINDIK QANATY
общественный фонд

INSTITUTE FOR WAR & PEACE REPORTING
IWPR
ИНСТИТУТ РЕПОРТАЖЕЙ ВОЙНЫ И МИРА