

ЦАХИМ ХӨГЖИЛ, ХАРИЛЦАА ХОЛБООНЫ
САЙДЫН ТУШААЛ

2024 оны ... сарын ... -ний өдөр

Дугаар

Улаанбаатар хот

ЖУРАМД НЭМЭЛТ ОРУУЛАХ ТУХАЙ

Монгол Улсын Засгийн газрын тухай хуулийн 24 дүгээр зүйлийн 2 дахь хэсэг, Монгол Улсын яамны эрхзүйн байдлын тухай хуулийн 8 дугаар зүйлийн 8.5 дахь хэсэг, Захиргааны ерөнхий хуулийн 68 дугаар зүйл, Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 25 дугаар зүйлийн 25.1.2 дахь заалтыг тус тус үндэслэн ТУШААХ нь:

1.Цахим хөгжил, харилцаа холбооны сайдын 2023 оны 09 дүгээр сарын 11-ний өдрийн А/90 дүгээр тушаалын хавсралтаар баталсан “Хүний эмзэг мэдээлэл, генетик болон биометрик мэдээлэл боловсруулахад баримтлах технологийн аюулгүй байдлын шаардлага, журам”-ын 3.1.5-д дор дурдсан агуулгатай заалт нэмсүгэй:

“3.1.5.эрүүл мэндийг хамгаалах, үйлчилгээ үзүүлэх зорилгоор хүний биометрик мэдээллийг ашиглахад мэдээллийн системдээ эрсдэлийн үнэлгээ хийлгэх;”.

2.Энэхүү тушаал батлагдсантай холбогдуулан журамд оруулсан нэмэлтийг зохих журмын дагуу захиргааны хэм хэмжээний актын улсын нэгдсэн бүртгэлд бүртгүүлэхийг тус яамны Кибер аюулгүй байдлын бодлогын хэрэгжилтийг зохицуулах газар (Э.Насанбат)-т даалгасугай.

САЙД

Н.УЧРАЛ

Цахим хөгжил, харилцаа холбооны сайдын
2024 оны ... дугаар сарын ...-ны өдрийн
... дугаар тушаалын хавсралт

Хүний эмзэг мэдээлэл, генетик болон биометрик
Мэдээлэл боловсруулахад баримтлах технологийн
Аюулгүй байдлын шаардлага, журам

Нэг.Нийтлэг үндэслэл

1.1.Энэхүү журмын зорилго нь Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 9, 10 дугаар зүйлд заасан хүний эмзэг мэдээлэл, генетик болон биометрик мэдээлэл (цаашид “мэдээлэл” гэх) боловсруулахад баримтлах зарчим, технологийн аюулгүй байдлын шаардлагыг тодорхойлоход оршино.

1.2.Хүний эмзэг мэдээлэл, генетик болон биометрик мэдээлэл боловсруулахтай холбоотой харилцаанд Хүний хувийн мэдээллийг хамгаалах тухай хууль, Кибер аюулгүй байдлын тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, тэдгээртэй нийцүүлэн гаргасан эрх зүйн акт болон энэхүү журмыг удирдлага болгоно.

1.3.Энэхүү журмын нэр томъёог Хүний хувийн мэдээлэл хамгаалах тухай хууль, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Кибер аюулгүй байдлыг хангах тухай хуульд заасантай нэгэн адил ойлгоно.

Хоёр.Мэдээлэл боловсруулахад баримтлах зарчим

2.1.Хүний эмзэг мэдээлэл, биометрик болон генетик мэдээллийг цуглуулах, боловсруулах, ашиглахад Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 5.1-д зааснаас гадна дараах зарчмыг баримтална:

- 2.1.1. ил тод байх;
- 2.1.2. зорилгодоо нийцсэн байх;
- 2.1.3. хадгалалтын хязгаарлалттай байх;
- 2.1.4. хариуцлагатай байх;
- 2.1.5. эрсдэлийн үнэлгээнд тулгуурласан байх;
- 2.1.6. мэдээллийн нэгдсэн системтэй байх.

Гурав.Технологийн аюулгүй байдлын шаардлага

3.1.Мэдээлэл боловсруулахад технологийн аюулгүй байдлын дараах шаардлагыг хангаж ажиллана:

3.1.1.мэдээлэл хариуцагч Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 20.1.1-д заасны дагуу баталсан дотоод журам баталж үйл ажиллагаандаа мөрдөж ажиллах;

3.1.2.мэдээлэл хариуцагч нь мэдээллийн аюулгүй байдлыг хангах нэгж, эсхүл хариуцсан ажилтантай байх;

3.1.3.мэдээлэл боловсруулах программ, сүлжээ, төхөөрөмж нь эрх бүхий этгээдээс зөвшөөрөгдсөн байх;

3.1.4.мэдээлэл хариуцагч нь мэдээлэл алдагдах, устах, гэмтэхээс урьдчилан сэргийлэх зорилгоор албан ёсны лицензтэй программ хангамж ашиглах, мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг хоёр жил тутамд, эсхүл шаардлагатай тохиолдолд тухай бүр хийлгэх;

3.1.5.эрүүл мэндийг хамгаалах, үйлчилгээ үзүүлэх зорилгоор хүний биометрик мэдээллийг ашиглахад мэдээллийн системдээ эрсдэлийн үнэлгээ хийлгэх;

3.1.6.мэдээлэл аюулгүй байдлын аудитыг жил тутамд, эсхүл аюулгүй байдал алдагдсан тохиолдол бүрд хийлгэх;

3.1.7.мэдээлэл хариуцагч нь мэдээллийг өөрчилсөн, устгасан, сэргээсэн тухай түүхчилсэн бүртгэлийг хөтөлж, хяналт тавин мэдээллийн бүрэн бүтэн, нууцлагдсан байдлыг хангах.

3.2.Мэдээлэл боловсруулах сервер нь дараах шаардлагыг хангасан байна:

3.2.1.Монгол Улсын нутаг дэвсгэрт байршдаг байх;

3.2.2.зөвхөн Монгол Улсаас нэвтрэх /хандах/ боломжтой байх;

3.2.3.зориулалтын техникийн өрөөнд серверийг байршуулсан байх;

3.2.4.шаардлагатай тохиолдолд серверийн хүчин чадлыг нэмэгдүүлэх боломжтой байх;

3.2.5.Төрийн мэдээлэл солилцооны “ХУР” системээр дамжуулан мэдээлэл солилцох боломжтой байх;

3.2.6.Харилцаа холбооны зохицуулах хорооны сүлжээний цагийн сервертэй холбогдсон байх;

3.2.7.мэдээлэл солилцох системийг “SSL” сертификатаар хамгаалсан байх;

3.2.8.тогтмол хугацаанд мэдээллийн системийг нөөцөлдөг байх.

3.3.Мэдээлэл боловсруулж буй этгээд сүлжээний аюулгүй байдлыг хангах зорилгоор сүлжээний орж, гарч байгаа урсгалуудыг тогтмол хянаж, сэжигтэй үйлдэл, хандалтыг зогсоох /firewall/ системтэй байна.

Дөрөв.Мэдээлэл боловсруулах ажиллагаанд тавих хяналт

4.1.Мэдээллийн эзэн өөрт хамааралтай мэдээллийг мэдээлэл хариуцагч боловсруулсан эсэх, мэдээллийг анхны зорилгоор боловсруулсан эсэхэд хяналт тавих эрхтэй.

4.2.Мэдээлэл хариуцагч нь мэдээллийн эзний тавьсан шаардлага, ирүүлсэн гомдол, саналыг холбогдох хуульд заасан хугацаанд, хуульд тусгайлан заагаагүй бол даруй шийдвэрлэж хариу өгөх үүрэгтэй.

---oOo---