ISO 27001 és 27002 kiterjesztése személyes adatok menedzselésével:

ISO/IEC 27701:2019

Móricz Pál – ügyvezető igazgató
Szenzor Gazdaságmérnöki Kft.

Szenzor
GAZDASÁGMÉRNÖKI KFT.

ISO 27000 szabványcsalád

27000 Áttekintés és szótár

27001
Követelmények

Útmutatók
27002 Code of practice
27003 Bevezetés
27037 Digitális bizonyíték
27038 Digitális redukció

27033-x Hálózat bizt
27034-x Alkalmazás bizt.
27036-x Szállító kapcs.

Auditorok, auditálás
27006 ISMS tanúsító köv.
27007 ISMS auditálás útmutató
27008 IS kontroll audit útmutató

Biztonság területek
27004 Mérés
27005 Kockázat mgmt
27035 Incidens mgmt
27031 Folytonosság
27032 Kiberbiztonság
27039 IDS
27040 Storage bizt.
27016 Szerv. gazdálk

Ágazatonkénti biztonság
27015 Pénzügyi szolg.
27011 for telecom
27010 Szervezetek közti komm.
27013 ISMS+ITSMS
27014 IS Governance
27019 Energiaipari foly. kontroll
27799 ISM eü-ben
27017 Cloud kontroll útmutató
27018 Public cloud sz.azon.info

Az új szabvány

ISO/IEC 27701:2019
Security technics – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guideline

(Biztonságtechnikák. Az ISO/IEC 27001 és ISO/IEC 27002 kiterjesztése a személyes adatok menedzsmentjével. Követelmények és útmutató)

Alkalmazási terület

PIMS – Privacy Information Management System

PII – Personally Identifiable Information (személyes adatok)

ISO/IEC 27701 PIMS követelmények és útmutató

27001 és 27002 kiegészítés

adatkezelőknek és adatfeldolgozóknak fejezetek

Szervezet méret, típus független
(aki PII-t kezel vagy dolgoz fel)

27001 követelmény kiegészítések (megfeleléshez) nem zárhatók ki

Tartalomjegyzék

Tartalomjegyzék - Mellékletek

Normatív mellékletek: PIMS-specifikus kontroll célok és kontrollok

A. PII kezelőknek

B. PII feldolgozóknak

Keresztreferencia mellékletek

C. ISO/IEC 29100 Adatvédelmi keretrendszer

D. GDPR

E. ISO/IEC 27018 cloud feldolgozó útmutató és ISO/IEC 29151 PII code practice

F melléklet: ISO/IEC 27701 alkalmazása

ISO/IEC 27001-re és ISO/IEC 27002-re

5. fejezet

Információbiztonság helyett *információbiztonság és személyes adatok védelme* (privacy), pl.

szervezet környezete, érdekelt felek elvárásaiban (szereptől függően),

menedzsment rendszer alkalmazási területében

kockázatok felmérésében, kezelésében

PIMS lehet külön és ISMS integrálva is

Alkalmazhatósági nyilatkozatban

adatkezelő és/vagy adatfeldolgozói kontrollok alkalmazására (7, 8 fejezetek illetve A és B melléklet) **is** ki kell térni (szereptől függően)

6. fejezet

további szempontok 27001/27002 kontrollokban pl.

politikák, szerepek felelősségek, tudatosság, képzés, információ osztályozás/jelölés, adathordozók kezelé-se/szállítása, berendezés selejtezés/újrahasznosítás, információ átadási, szállítói, titoktartási megállapodások, alkalmazás-szolgáltatás nyilvános hálózatokon, titkosítás, fejlesztési elvek, jogi követelmények, feljegyzések védelme, átvizsgálások, stb.

felhasználó regisztrációs, hozzáférési, bejelentkezési rendszer

mentés, naplózás, napló védelem

incidenskezelés

7. fejezet, A melléklet

7. További kontroll célok és kontrollok (kontroll, bevezetési útmutató, további útmutató)

adatkezelőknek

7.2 adatgyűjtés, adatkezelés feltételei:

cél azonosítás és dokumentálás,

jogalap,

mikor, hogyan nyerjük hozzájárulást

hozzájárulás megszerzés és feljegyzés

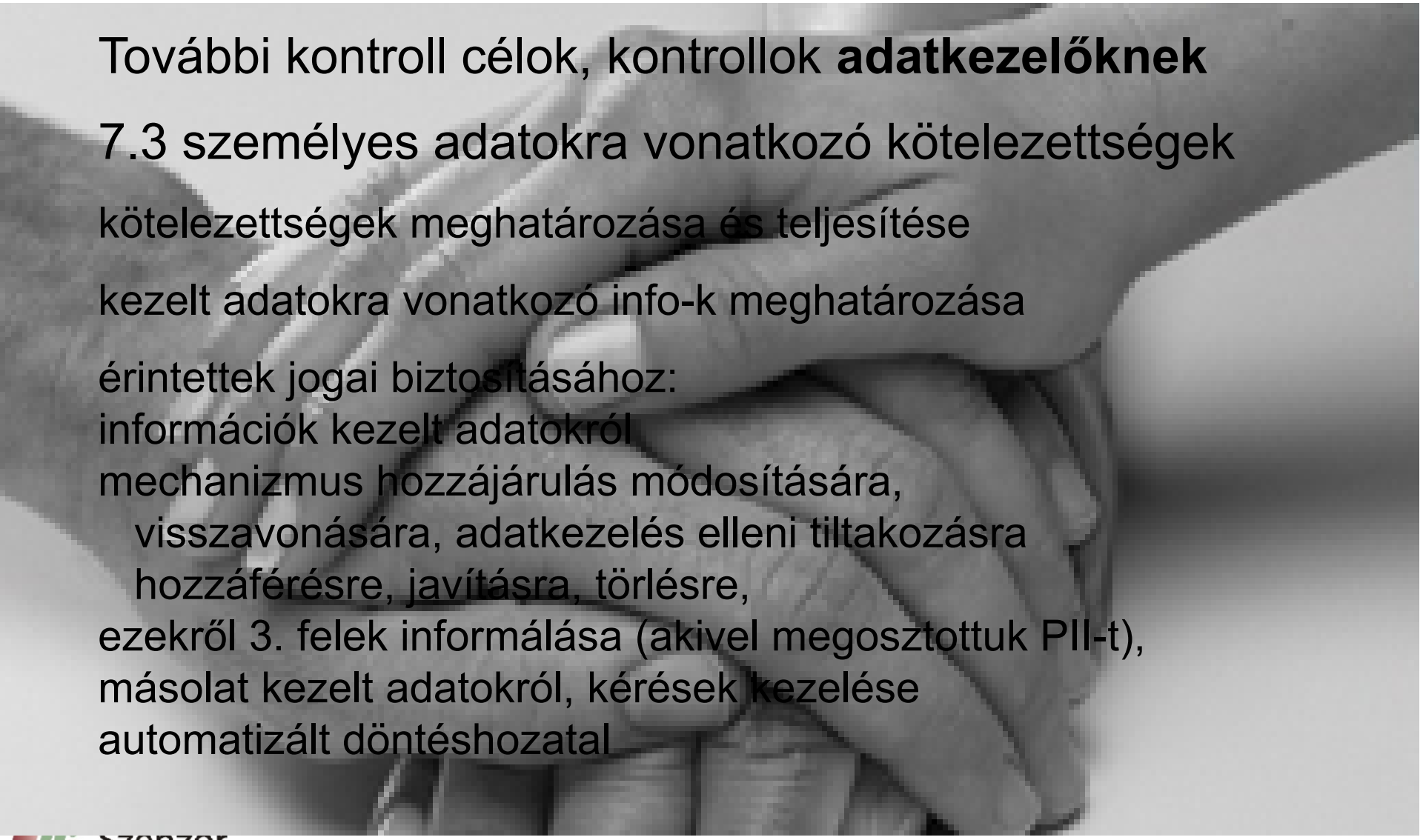
hatásfelmérés,

szerződés adatfeldolgozókkal

közös adatkezelés,

adatkezeléshez kapcsolódó feljegyzések

7. fejezet, A melléklet



További kontroll célok, kontrollok **adatkezelőknek**

7.3 személyes adatokra vonatkozó kötelezettségek

kötelezettségek meghatározása és teljesítése

kezelt adatokra vonatkozó info-k meghatározása

érintettek jogai biztosításához:
információk kezelt adatokról
mechanizmus hozzájárulás módosítására,
visszavonására, adatkezelés elleni tiltakozásra
hozzáférésre, javításra, törlésre,
ezekről 3. felek informálása (akivel megosztottuk PII-t),
másolat kezelt adatokról, kérések kezelése
automatizált döntéshozatal

7. fejezet, A melléklet

További kontroll célok és kontrollok **adatkezelőknek**

7.4 Beépített, alapértelmezett védelem
(privacy by design and privacy by default)

korlát gyűjtésre, feldolgozásra, pontosság és minőség, adat minimalizálás, anonimizálás/törlés a feldolgozás végén, ideiglenes fájlok kezelése, megőrzés, eltávolítás, adat átadás felügyelet

7.5 PII megosztás, átadás és kiadás

átadás jogi alapjainak azonosítása,

országok, nemzetközi szervezetek, amelyeknek PII-t átadhatnak,

feljegyzések az átadásról

feljegyzés 3. félnek (pl. hatóság) kiadásról

8. fejezet, B melléklet

8. További kontroll célok és kontrollok **adatfeldolgozóknak**

8.2 Adatgyűjtés és –kezelés feltételei

vevői megállapodás („feldolgozói szerződés”)

szervezeti célok (csak ami szerződésben)

használat marketingre és hirdetésre (csak hozzájárulá

jogsértő használat (vevő informálás)

vevői kötelezettségek (info nyújtás hozzá)

kezeléshez kapcsolódó feljegyzések

8.3 PII-re vonatkozó kötelezettségek

vevői kötelezettségek teljesítéséhez kapcsolódó feldolgozói feladatok elvégzése

8. fejezet, B melléklet

További kontroll célok, kontrollok **(adatfeldolgozók)**

8.4 Beépített és alapértelmezett védelem

ideiglenes fájlok, PII visszaadás, átadás, kiadás, adatátadás felügyelet

8.5 PII megosztás, átadás és kiadás

átadás jogi alapjainak azonosítása,

országok, nemzetközi szervezetek, amelyeknek PII-t átadhatnak,

feljegyzés 3. félnek (pl. hatóság) kiadásról, kiadási kérések bejelentése (vevőnek), joghoz kötése

adatokat kezelő alvállalkozó igénybe vétel, változás előtti vevő tájékoztatása, elvárások alvállalkozótól vevői megállapodással összhangban

Tanúsítás

GDPR

Adatkezelői/adatfeldolgozói kötelezettség, beépített és alapértelmezett védelem, adatbiztonság (technikai és szervezési intézkedések)
„teljesítést bizonyíthatja (ehhez felhasználható) tanúsítási mechanizmushoz csatlakozás”

követelmények tanúsító szervezetre, folyamatra

2011 CXII (info) tv 69§:

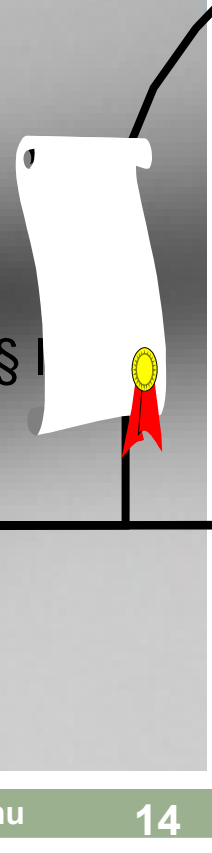
GDPR tanúsítást NAIH végzi

2015 CXXIV (akkreditációs) tv

adatvédelmi tanúsító akkreditálási kérelmet NAH-nak nyújthat be (10§ l
ehhez

vannak akkreditációs szabványok,
kell akkreditációs séma,

sémának, GDPR követelményeknek megfelelés



Elérhetőség

Móricz Pál **Mobil: 20-931-0584**

p.moricz@szenzor-gm.hu

Szenzor Gazdaságmérnöki Kft.

1087 Budapest, Könyves Kálmán körút 76.

Telefon: (+36)-1-331-5523

Fax: (+36)-1-311-9636

E-mail: szenzor@szenzor-gm.hu

Honlap: www.szenzor-gm.hu

„Változással a sikerért”