Informationssikkerhed og privatlivsbeskyttelse

ISO 27001 & ISO 27701

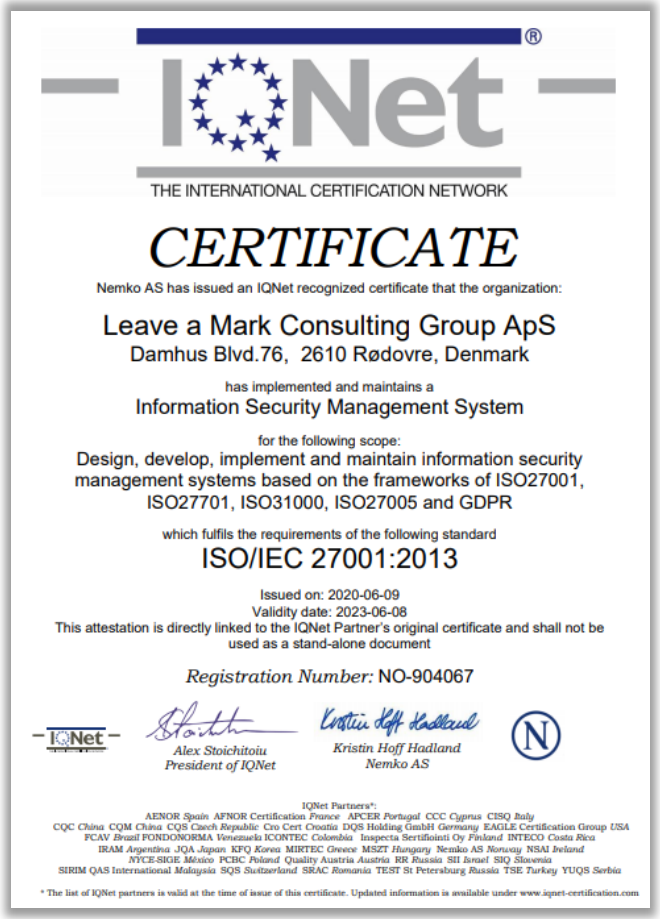
Aarhus, 11 JUNI 2020

leaveamarkgroup.com

LEAVE A MARK
CONSULTING GROUP

LEAVE
A MARK
CONSULTING GROUP

- Leave a Mark Consulting Group hjælper til daglig virksomheder med at opnå compliance og certificering inden for informationssikkerhed.
- Leave a Marks konsulenter er alle certificeret indenfor it- og informationssikkerhed
- Leave a Mark er ISO 27001 certificeret inkl. ISO 27701



IQNet®

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

Nemko AS has issued an IQNet recognized certificate that the organization:

Leave a Mark Consulting Group ApS
Damhus Blvd.76, 2610 Rødovre, Denmark

has implemented and maintains a
Information Security Management System

for the following scope:
Design, develop, implement and maintain information security management systems based on the frameworks of ISO27001, ISO27701, ISO31000, ISO27005 and GDPR

which fulfils the requirements of the following standard
ISO/IEC 27001:2013

Issued on: 2020-06-09
Validity date: 2023-06-08
This attestation is directly linked to the IQNet Partner's original certificate and shall not be used as a stand-alone document

Registration Number: NO-904067

IQNet — Alex Stoichitoiu, President of IQNet — Kristin Hoff Hadland, Nemko AS

IQNet Partners*:
AENOR *Spain* AFNOR Certification *France* APCER *Portugal* CCC *Cyprus* CISQ *Italy*
CQC *China* CQM *China* CQS *Czech Republic* Cro Cert *Croatia* DQS Holding GmbH *Germany* EAGLE Certification Group *USA*
FCAV *Brazil* FONDONORMA *Venezuela* ICONTEC *Colombia* Inspecta Sertifiointi Oy *Finland* INTECO *Costa Rica*
IRAM *Argentina* JQA *Japan* KFQ *Korea* MIRTEC *Greece* MSZT *Hungary* Nemko AS *Norway* NSAI *Ireland*
NYCE-SIGE *México* PCBC *Poland* Quality Austria *Austria* RR *Russia* SII *Israel* SIQ *Slovenia*
SIRIM QAS International *Malaysia* SQS *Switzerland* SRAC *Romania* TEST St Petersburg *Russia* TSE *Turkey* YUQS *Serbia*

* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

leaveamarkgroup.com

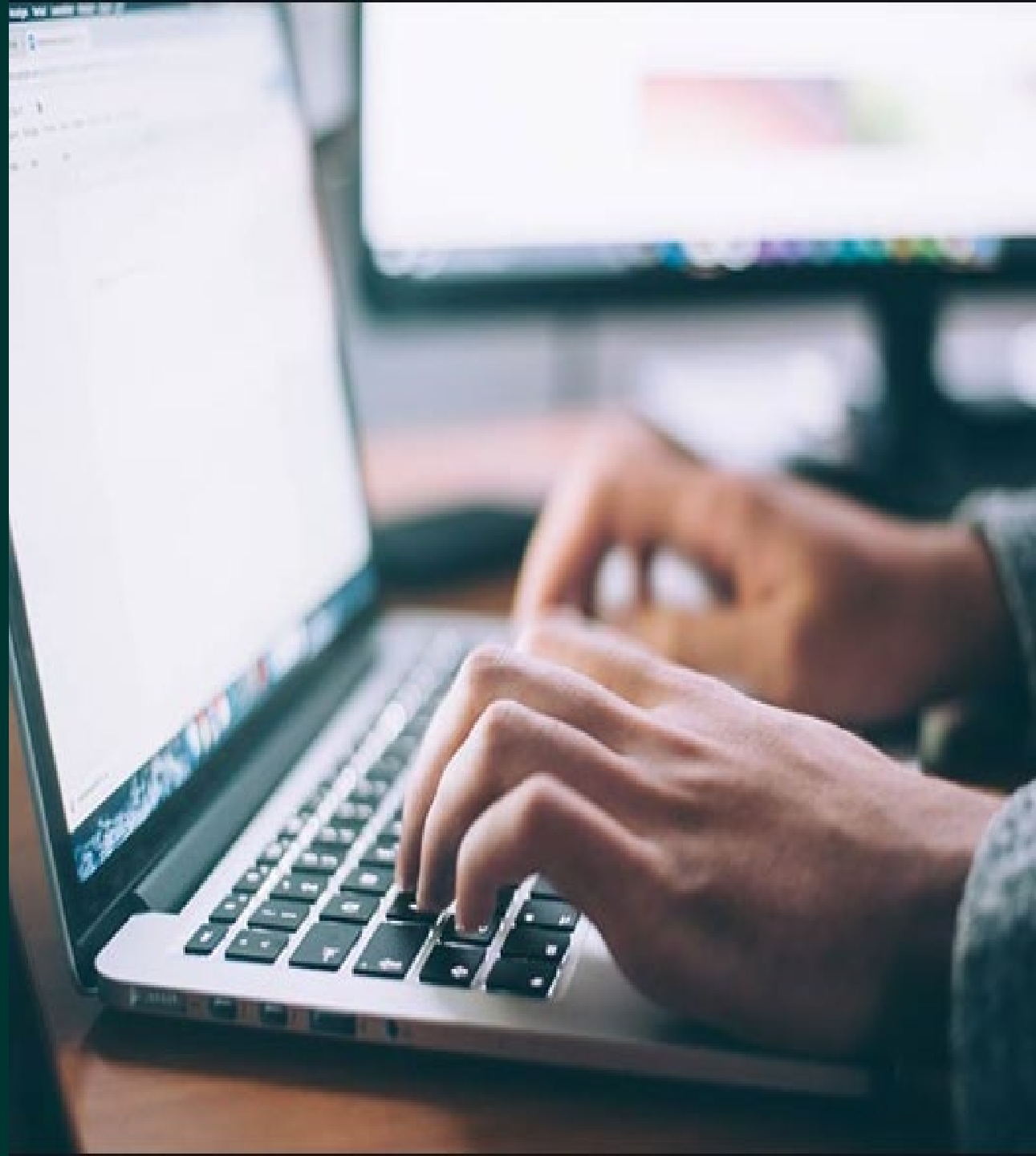
ISO 27701
A
Privacy Information Management System (PIMS)

ISO 27701

Er standarden for privatlivsbeskyttelse.

ISO 27701, er et ledelsessystem (PIMS), som sikre arbejdsgange og foranstaltninger, for at opnå en passende beskyttelse af personoplysninger.

Standarden er en udvidelse af ledelsesstandarden ISO 27001 for informationssikkerhed.



ISMS + PIMS Scope

PIMS
ISO 27701
Privatliv

ISMS
ISO 27001
Integritet, tilgængelighed, fortrolighed

Husk! at selv om man indfører ISO 27701 så er det ikke sikkert at man overholder persondataforordningen

- *medmindre* man designer den til det.

LEAVE A MARK
CONSULTING GROUP

Nye tiltag ved udvidelse med ISO 27701

Nye områder f.eks.

- Betingelser for indsamling og behandling
- Forpligtelser over for de registrerede
- Privacy by design and privacy by default
- Deling, overførsel og videregivelse af personoplysninger

Nye begreber også i forhold til GDPR f.eks.

- PII controller – data ansvarlig
- PII processor – data behandler
- PII principal – Data subjekt

Nye data klassificeringer fra GDPR

- Almindelige oplysninger
- Særlige kategorier (følsomme)
- Fortrolige oplysninger (strafbare forhold)

ISO/IEC 27701:2019 Annex A controls		
Clause	**Sec**	**Control Objective/Control**
A 7.2 Conditions for collection and processing	A.7.2.1	Identify and document the purpose
	A.7.2.2	Identify lawful basis
	A.7.2.3	Determine when and how consent is to be obtained
	A.7.2.4	Obtain and record consent
	A.7.2.5	Privacy impact assessment
	A.7.2.6	Contracts with PII processors
	A.7.2.7	Joint PII controller
	A.7.2.8	Records related to processing PII

Kilde: ISO/IEC 27701:2019

LEAVE A MARK
CONSULTING GROUP

Hvilke områder har ISO 27701 indflydelse på?

- Organisering af informationssikkerhed
  - *Governance, framework, strategi* etc
- Personalesikkerhed
- Styring af aktiver
  - *Risikovurdering*
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Styring af informationssikkerhedsbrud og forbedringer
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Overensstemmelse med lov- og kontraktkrav

ALLE OMRÅDER kan være berørt

LEAVE A MARK
CONSULTING GROUP

Hvad gjorde vi?

LEAVE A MARK
CONSULTING GROUP

Krav til implementering af ISO 27701

(I henhold til LAM´s forretningsstrategi/risiko appetit)

- Skal understøtte LAM’s forretningsstrategi fremadrettet
- Skal være en del af daglige processer
- Skal ikke kræve ekstra tid at vedligeholde (i forhold til ISO 27001)
- Skal sikre robusthed
- Skal implementeres som en del af LAM’s FastTrack model/framework
- Skal være baseret på risikovurdering

LEAVE A MARK
CONSULTING GROUP

Leave a Mark's proces

Forretningsstrategi + risiko appetit

Scope
ISO 27701 SOA

Risikovurdering

Opdatering af politikker og procedure

Opdatering af foranstaltninger og kontroller

Intern audit

Extern audit

Alle processer, documenter mm er håndteret i LAM's FastTrack Framework

Benspænd

Nummeringen stemmer ikke 1:1 mellem standarderne.

Konsekvens for individet
Overvurdering eller undervurdering?

Flere ”hatte” i SMV´er

Det er ofte de samme der har flere roller

Det er mere omfattende end forventet – alt i alt

”

Say it, do it, prove it !

LEAVE
A MARK
CONSULTING GROUP

Erfaringer

- Det kan lade sig gøre for en lille virksomhed at blive certificeret!
- En af udfordringerne var at få ISO 27701 ind som en naturlig del af ISO 27001 – ”det skal tænkes rigtigt” så det ikke bliver en ekstra byrde.
- Ca. 30% af de eksisterende politikker i ISO 27001 blev udvidet ved ISO 27701 (er virksomhed afhængig).
- ISO 27701 gav struktureret tilgang til implementeringen.
- Samlede kontroller gjorde arbejdet lettere og gav højere kvalitet.
- Risikobaseret tilgang hjalp på prioriteringen og holder omkostninger/tidsforbrug nede.
- Optimeringspotentiale for processer og systemer blev synlige.
- Nemmere dialog med potentielle kunder.

LEAVE A MARK
CONSULTING GROUP

Spørgsmål?

LEAVE A MARK
CONSULTING GROUP

Helle Friborg

CEO

leaveamarkgroup.com

(+45) 535 27000

helle.friborg@leaveamarkgroup.com

linkedin.com/in/helle-friborg-7581a32