AVVERA

2024 NEWSLETTER Ottobre

La Commissione Europea conclude il primo riesame del Data Privacy Framework con gli Stati Uniti

Protezione dei consumatori nell'era dell'IA: la Commissione UE adotta due proposte normative

Obblighi del titolare in caso di nomina di un responsabile

L'ITL deve rifiutare l'autorizzazione al datore di lavoro non titolare

L'Autorità Garante pone l'accento sul controllo nei confronti dei Responsabili nominati

Il Garante sanziona ancora sulla non corretta gestione delle mail

Parere del Garante privacy francese su un nuovo progetto di "age verification"

SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

IMQ CERTIFIED QUALITY MANAGEMENT SYSTEM ISO 9001:2015
IMQ CERTIFIED OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM ISO 45001:2018
IMQ CERTIFIED INFORMATION SECURITY MANAGEMENT SYSTEM ISO/IEC 27001:2013

La Commissione Europea conclude il primo riesame del Data Privacy Framework con gli Stati Uniti

Nella sua decisione sull'adeguatezza del 10 luglio 2023, la Commissione ha constatato che il Data Privacy Framework (DPF) fornisce un livello di protezione adeguato per i dati personali trasferiti dall'Unione Europea ad organizzazioni negli Stati Uniti d'America. Il Considerando 211 della decisione di adeguatezza prevedeva anche che la Commissione effettuasse revisioni periodiche, la prima delle quali doveva avvenire dopo un anno dalla data di notifica della decisione di adeguatezza agli Stati membri.

In data 9 Ottobre 2024, la Commissione concludeva questo primo esame, presentando il proprio rapporto.

Il rapporto si concentra sulla verifica dell'attuazione e del funzionamento efficace di tutti gli elementi previsti dal Data Privacy Framework. Il riesame ha riguardato tutti gli aspetti del funzionamento del quadro, anche alla luce degli sviluppi giuridici intervenuti dopo l'adozione della decisione di adeguatezza.

Sulla base delle informazioni raccolte durante questo primo esame, la Commissione conclude che le autorità statunitensi hanno messo in atto le strutture e le procedure necessarie per garantire il funzionamento efficace del Data Privacy Framework, rimarcando la collaborazione delle autorità statunitensi per condurre la revisione.

La Commissione rileva, in ogni caso, che l'esperienza dell'applicazione pratica delle salvaguardie che si applicano sia al trattamento dei dati personali da parte delle aziende certificate sia all'accesso ai dati da parte delle autorità pubbliche è necessariamente limitata dopo un solo anno di funzionamento. Quindi, la Commissione intende monitorare gli sviluppi pertinenti nel corso dei prossimo periodo, prestando particolare attenzione a:

1. le prossime relazioni del Privacy and Civil Liberties Oversight Board (PCLOB) sull'attuazione della EO 14086 e sul funzionamento del meccanismo di ricorso;
2. possibili ulteriori modifiche della Sezione 702 del Foreign Intelligence Surveillance Act (FISA);
3. la nomina di membri del PCLOB per coprire i posti vacanti.

Inoltre, per garantire un funzionamento continuo ed efficace, la Commissione ha ritenuto fondamentale che:

- il Dipartimento del Commercio statunitense faccia un uso più completo dei diversi strumenti forniti dal Data Privacy Framework per il monitoraggio della conformità delle aziende ai principi del DPF e per l'individuazione di false dichiarazioni di partecipazione;
- la Federal Trade Commission (FTC) si impegni ad avere un approccio proattivo alle indagini e all'applicazione della conformità ai principi del DPF da parte delle aziende statunitensi certificate;

This document is confidential to Avvera and is subject to copyright protection

- il Dipartimento del Commercio, la FTC e le autorità di protezione dei dati dell'Unione Europea sviluppino strumenti di orientamento comuni sui requisiti chiave dei principi del DPF, in particolare, sulle tematiche dei trattamenti di dati personali nell'ambito delle risorse umane e dei trasferimenti effettuati successivi *(onward transfers).*

Sul tema del onward transfers, i principi del DPF prevedono che possono essere effettuati:
- solo per scopi limitati e specifici;
- sulla base di un accordo scritto tra l'organizzazione DPF UE-USA e la terza parte;
- solo se tale contratto prevede che la terza parte fornisca lo stesso livello di protezione.

Alla luce dei risultati del riesame, la Commissione ha ritenuto opportuno effettuare il prossimo riesame periodico dopo tre anni e consulterà il Comitato europeo per la protezione dei dati (EDPB) in merito alla periodicità dei futuri riesami.

This document is confidential to Avvera and is subject to copyright protection

Protezione dei consumatori nell'era dell'IA: la Commissione UE adotta due proposte normative

La Commissione Europea, con un comunicato stampa dello scorso 28 settembre, ha annunciato l'adozione di due proposte finalizzate ad aggiornare le normative sulla responsabilità per prodotti, nonché relative all'intelligenza artificiale (IA), adeguandole alle correnti esigenze dell'era digitale.

Le norme attuali dell'UE sulla responsabilità per danno da prodotti difettosi, basate sulla responsabilità oggettiva dei fabbricanti, risalgono a quasi 40 anni fa. Pertanto, secondo quanto riportato, è essenziale aggiornare le normative sulla responsabilità per supportare la trasformazione verde e digitale, assicurando certezza giuridica alle imprese e una protezione adeguata ai consumatori, specialmente di fronte alle sfide poste dalle nuove tecnologie.

Uno degli aspetti chiave delle nuove regole è il mantenimento della responsabilità oggettiva dei produttori. In questo modo, le aziende che producono o distribuiscono beni, compresi i prodotti basati su tecnologie avanzate, continueranno ad essere responsabili dei danni causati da difetti, come lesioni personali, danni materiali o perdita di dati. Questo vale anche per i prodotti che diventano pericolosi a seguito di aggiornamenti software o di problemi legati alla sicurezza informatica.

Inoltre, la Commissione UE intende armonizzare le normative nazionali sulla responsabilità legata all'intelligenza artificiale, rendendo più semplice ottenere un risarcimento per chi ha subito danni dall'uso di sistemi basati su IA. Ad esempio, i consumatori europei potranno richiedere risarcimenti anche per danni causati da prodotti importati da paesi terzi, creando condizioni eque tra produttori locali e internazionali.

L'obiettivo è creare un ambiente di fiducia per i consumatori, senza frenare l'innovazione tecnologica, ma anzi consentendo alle aziende di investire in nuove tecnologie con la certezza di operare in un quadro legale chiaro e trasparente.

Le proposte legislative dovranno essere approvate dal Parlamento europeo e dal Consiglio, un processo che definirà le tappe future di implementazione. Inoltre, la Commissione precisa che si impegnerà a valutare l'efficacia delle nuove normative sull'IA entro cinque anni dall'entrata in vigore, per decidere se introdurre ulteriori regole di responsabilità oggettiva.

This document is confidential to Avvera and is subject to copyright protection

Obblighi del Titolare in caso di nomina di un Responsabile

Con una nota stampa rilasciata lo scorso 9 ottobre l'European Data Protection Board – EDPB ha informato che nel corso dell'ultima sessione plenaria è stato adottato un parere su alcuni obblighi derivanti dal ricorso a responsabili del trattamento e sub-responsabili del trattamento.

L'EDPB ha ricordato che, con riferimento agli obblighi derivanti dall'affidamento ai responsabili del trattamento e ai sub-responsabili del trattamento, i titolari del trattamento sono onerati da determinati doveri dei titolari del trattamento derivanti in particolare dall'articolo 28 GDPR. L'EDPB ha analizzato questi doveri, in particolare concentrandosi sui seguenti aspetti.

L'EDPB spiega che i titolari del trattamento dovrebbero avere le informazioni sull'identità (ossia nome, indirizzo, persona di contatto) di tutti i responsabili del trattamento, sub-responsabili del trattamento ecc. prontamente disponibili in ogni momento.

Inoltre l'obbligo del titolare del trattamento di verificare se i (sub)responsabili del trattamento presentino "garanzie sufficienti" dovrebbe applicarsi indipendentemente dal rischio per i diritti e le libertà degli interessati, sebbene la portata di tale verifica possa variare sulla base dei rischi associati al trattamento. Sempre nell'ambito delle verifiche dovute in capo al titolare, non esiste secondo l'EDPB un elenco di controlli da porre in essere, ma è chiaro che l'obbligo è continuativo nel tempo (quindi non da limitare alla fase di scelta).

L'EDPB afferma anche che, mentre il responsabile del trattamento iniziale dovrebbe garantire di proporre sub-responsabili del trattamento con garanzie sufficienti, la decisione finale e la responsabilità sull'assunzione di uno specifico sub-responsabile del trattamento spettano al titolare del trattamento.

L'EDPB ritiene che, ai sensi del GDPR, il titolare del trattamento non abbia il dovere di chiedere sistematicamente ai contratti di nomina del sub responsabile per verificare se gli obblighi in materia di protezione dei dati sono stati trasmessi lungo la catena di trattamento. Il titolare del trattamento dovrebbe valutare se la richiesta di una copia di tali contratti o il loro riesame siano necessari per poter dimostrare la conformità al GDPR. Con riferimento all'obbligo in capo al responsabile di imporre i medesimi obblighi che il titolare gli ha imposto anche sui sub responsabili, l'EDPB ha specificato che tali obblighi non devono essere intesi assolti solo qualora sia stata usata la stessa formulazione.

In caso di trasferimenti di dati personali al di fuori dello Spazio economico europeo avvengano tra due (sub)

This document is confidential to Avvera and is subject to copyright protection

responsabili del trattamento, l'EDPB prescrive che il responsabile del trattamento – in quanto esportatore di dati – dovrebbe preparare la documentazione pertinente, ad esempio relativa al motivo del trasferimento utilizzato, alla valutazione d'impatto del trasferimento e alle eventuali misure supplementari.
Tuttavia, poiché il titolare del trattamento è ancora soggetto agli obblighi derivanti dall'articolo 28, paragrafo 1, GDPR in materia di "garanzie sufficienti", oltre a quelli di cui all'articolo 44 per garantire che il livello di protezione non sia compromesso dai trasferimenti di dati personali, dovrebbe valutare tale documentazione ed essere in grado di mostrarla all'autorità di protezione dei dati competente.

This document is confidential to Avvera and is subject to copyright protection

L'ITL deve rifiutare l'autorizzazione al Datore di Lavoro non Titolare

L'Ispettorato Nazionale del Lavoro ha trasmesso una nota (rif. nota 7020/2024 del 25 settembre 2024) alle direzioni interregionali e agli ispettorati territoriali per chiarire che non è possibile rilasciare un provvedimento autorizzativo, disciplinato dall'articolo 4 dello Statuto dei lavoratori (legge 300/1970), nelle ipotesi in cui il titolare dei dati personali acquisiti mediante strumenti dai quali può incidentalmente derivare un controllo a distanza non coincida con il datore istante, ma sia un soggetto terzo estraneo al rapporto di lavoro.

La nota fa riferimento ai casi in cui sono ad esempio installati:
- impianti di videosorveglianza presso negozi in franchising sulla base della richiesta del franchisor e non per esigenze del datore di lavoro che gestisce il singolo punto vendita, o
- impianti di geolocalizzazione su veicoli sulla base del committente del servizio di trasporto e non per finalità proprie della società vettore prestatrice del servizio stesso.

Sul tema l'Ispettorato Nazionale del Lavoro ha rilevato che:
- nella documentazione tecnica allegata all'istanza spesso non è chiaro chi ricopra effettivamente i ruoli di Titolare del trattamento e di Responsabile del trattamento dei dati desunti dai suddetti sistemi, o/ e
- si evince in maniera chiara che il Titolare del trattamento di fatto è la società committente e non il vettore/ datore di lavoro.

L'Ispettorato Nazionale del Lavoro, formulando una proposta di riscontro che le sedi territoriali devono rendere in tali circostanze, non manca di sottolineare che l'impossibilità di emettere l'autorizzazione va a discapito della possibilità di fare riferimento a tale atto quale elemento del bilanciamento di interessi che legittima il trattamento di dati personali dei lavorati.

This document is confidential to Avvera and is subject to copyright protection

L'Autorità Garante pone l'accento sul controllo nei confronti dei Responsabili Nominati

L'Autorità Garante, con proprio Provvedimento del 17 luglio 2024 [doc. web n. 10053211], ha sanzionato un'importante società che opera nel settore della vendita a clienti finali di energia elettrica e gas, in particolare, a causa dell'illecito trattamento posto in essere dalla società quale Titolare, per il tramite di alcune agenzie designate Responsabili (ex art. 28 del Reg. UE 2016/679 "GDPR") delle attività di trattamento, che hanno finalizzato numerose attivazioni di contratti non richiesti.

Nel corso dell'istruttoria il Garante ha rilevato che sebbene i trattamenti illeciti siano stati posti in essere da Responsabili ex art. 28 GDPR, che hanno operato in qualità di agenti in violazione delle disposizioni impartite dal titolare, le misure tecniche e organizzative adottate dal titolare nell'ambito del processo di acquisizione della clientela per il tramite dell'agenzia, non erano adeguate alla natura, al contesto, alle finalità e ai rischi del suddetto trattamento, così configurando in capo al Titolare una violazione del principio di accountability (art. 5, par. 1, let. f) e art. 24 del GDPR).

L'Autorità ha evidenziato che secondo tale principio, **al Titolare è attribuita la responsabilità generale del trattamento posto in essere direttamente o da altri per suo conto, gravando, pertanto, sullo stesso l'onere di attuare un sistema organizzativo contraddistinto da efficaci misure di protezione dei dati personali.**

A tal fine, l'Autorità ha chiarito come oltre alla predisposizione degli adempimenti normativi (tra cui: informativa, registro delle attività di trattamento, nomina del responsabile della protezione dei dati ove obbligatoria, valutazione di impatto ove necessario, ecc.), il Titolare debba implementare procedure e prassi organizzative atte a conformare i relativi trattamenti al GDPR, tra cui:

- processi di mappatura dei trattamenti;
- regole per l'attribuzione di responsabilità;
- programmi di formazione del personale;
- procedure per la verifica dell'operato dei responsabili designati ai sensi dell'art. 28;
- previsione di audit interni ed esterni con cadenza periodica.

Nel caso in esame, l'Autorità ha rilevato come il Titolare non avesse implementato adeguate procedure e prassi, omettendo di fornire indicazioni dettagliate sulle modalità di raccolta dei dati personali dei clienti e lasciando agli agenti eccessiva autonomia. Tale mancanza ha comportato l'acquisizione, da parte degli agenti, di copia dei documenti d'identità anche tramite fotografie scattate con il dispositivo mobile personale dell'agente, così consentendo che la documentazione fosse nella piena disponibilità dell'agente e esponendo al rischio che fosse utilizzata da quest'ultimo per il compimento di attività illecite, nell'ambito dell'attivazione di contratti non richiesti.

This document is confidential to Avvera and is subject to copyright protection

Ma non solo, l'Autorità ha ravvisato l'inadeguatezza anche della fase di verifica della volontà negoziale, tramite chiamata di conferma (c.d. "quality call") al numero di telefono indicato nella proposta contrattuale. Ed invero, l'irreperibilità del contraente, nella maggior parte dei casi, non interrompeva il processo di contrattualizzazione.

Anche l'invio della welcome letter all'indirizzo e-mail o fisico indicato dal cliente nella fase di sottoscrizione del contratto, era basato unicamente su dati acquisiti dall'agente, senza alcuna possibilità di verifica della corrispondenza degli stessi con quelli dell'effettivo utilizzatore dell'utenza.

Per quanto esposto l'Autorità ha comminato la sanzione amministrativa di euro 5.000.000,00 a Hera Comm S.p.A. e imposto una serie di misure correttive.

Va rilevato che tale provvedimento si pone in linea con la recente Opinion dell'European Data Protection Board (7 ottobre 2024) sugli obblighi dei titolari del trattamento in relazione ai responsabili, che ha rafforzato i doveri disposti dall'art. 28 del GDPR in capo ai Titolari del trattamento.

This document is confidential to Avvera and is subject to copyright protection

Il Garante sanziona ancora sulla non corretta gestione delle mail

Con il provvedimento n. 472/2024 del 17 luglio 2024 il Garante per la protezione dei dati personali ha sanzionato una società con una multa di €80.000 per violazione dei principi del GDPR, dovuta al **trattamento illegittimo tramite un software di gestione e archiviazione sistematica delle mail** (compreso backup delle stesse).

La vicenda origina da un reclamo presentato da un ex collaboratore della società, il quale lamentava un trattamento illecito dei propri dati personali, riconducibile alla gestione della casella di posta elettronica aziendale a lui assegnata durante il rapporto di collaborazione. L'indagine del Garante ha evidenziato come la società conservasse i backup delle email dei collaboratori per un periodo prolungato – fino a tre anni – dalla cessazione del rapporto lavorativo. Tale pratica è risultata in contrasto con il principio di minimizzazione, sancito dall'articolo 5, paragrafo 1, lettera c), del GDPR, poiché il periodo di conservazione eccedeva le finalità dichiarate e non era adeguatamente giustificato rispetto alle esigenze di continuità aziendale.

Successivamente, il Garante ha analizzato l'informativa condivisa dalla società rilevando la violazione degli obblighi di trasparenza e liceità del trattamento previsti dall'articolo 5, paragrafo 1, lettera a), e dall'articolo 13 del GDPR. In particolare, l'informativa ometteva dettagli relativi alle modalità del trattamento – limitandosi a menzionare genericamente la possibilità di accesso alla casella di posta per esigenze di sicurezza informatica e continuità operativa – senza specificare i tempi di retention dei backup delle email successivi alla cessazione del rapporto lavorativo.

In ultima analisi, sotto al profilo giuslavoristico l'utilizzo di questa soluzione software "aggiuntiva" sollevava questioni sotto il profilo del controllo a distanza sui lavoratori, ai sensi dell'articolo 4 dello Statuto dei Lavoratori (Legge n. 300/1970), richiamato dall'articolo 114 del Codice Privacy. Secondo tale disciplina, l'impiego di strumenti che permettono un controllo indiretto dell'attività lavorativa è consentito solo previo accordo con le rappresentanze sindacali aziendali o autorizzazione dell'Ispettorato del lavoro. L'utilizzo del software per il backup delle email, senza l'adozione delle citate garanzie, comportava un potenziale monitoraggio delle attività lavorative, poiché il sistema permetteva di conservare i dati, trattare il contenuto della posta elettronica che transitava sugli account aziendali, e infine accedere ai log di accesso alle caselle di posta e al gestionale in uso ai dipendenti (metadati che venivano conservati per un periodo di 6 mesi).

Appare evidente che questa raccolta poteva quindi consentire alla società sia di ricostruire l'attività dei collaboratori attraverso l'analisi delle comunicazioni sia di mappare i metadati relativi agli accessi, offrendo una ricostruzione dettagliata dell'attività lavorativa dei dipendenti – anche oltre la cessazione del rapporto – risultando così ecces-

This document is confidential to Avvera and is subject to copyright protection

siva e non proporzionata rispetto al conseguimento delle finalità dichiarate (di sicurezza della rete informatica e di continuità dell'attività aziendale) e trasformando potenzialmente il software in uno strumento di potenziale controllo a distanza.

Il Garante criticando il sistema di back-up delle caselle di posta elettronica aziendale, ha affermato che *"per assicurare l'ordinario svolgimento e la continuità dell'attività aziendale, è necessario predisporre sistemi di gestione documentale in grado di archiviare e conservare i documenti "con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile" e che tali caratteristiche "non possono rinvenirsi nei sistemi di posta elettronica che, infatti, rispondono ad altre finalità".*

In esito alla propria istruttoria, l'Autorità ha comminato alla società una sanzione amministrativa di €80.000, calcolata tenendo conto delle gravi carenze riscontrate, nonché dell'assenza di precedenti specifici a carico della società e della sua collaborazione per conformarsi alle indicazioni dell'Autorità sospendendo l'utilizzo del software. Il Garante ha altresì disposto il divieto di ulteriore trattamento dei dati estratti tramite il software.

Dal provvedimento emerge quindi, ancora una volta, l'esigenza per i titolari di indicare sempre in sede di informativa ai propri collaboratori le finalità del trattamento assieme la limitazione del periodo di conservazione dei dati personali in maniera puntuale e specifica in modo da non incorrere in eventuali sanzioni.

This document is confidential to Avvera and is subject to copyright protection

Parere del Garante Privacy francese su un nuovo progetto di "Age Verification"

Con Deliberazione n. 2024-067 del 26 settembre 2024, la CNIL, l'Autorità garante francese per la protezione dei dati personali, ha espresso un parere sul quadro di disciplina dell'Autorità francese di Regolamentazione della Comunicazione Audiovisiva e Digitale (ARCOM) riguardante i sistemi di verifica dell'età per accedere a contenuti pornografici online. Questo quadro mira a stabilire i requisiti tecnici minimi per i sistemi di verifica dell'età che consentono l'accesso a servizi di comunicazione pubblica online e piattaforme di condivisione video che rendono disponibili contenuti pornografici.

La CNIL ha chiarito che la Legge francese n. 2024-449 del 21 maggio 2024 consente all'ARCOM di operare questi interventi e di imporre sanzioni finanziarie, previa consultazione con la CNIL stessa. Inoltre, la Legge francese n. 2020-936 del 30 luglio 2020, che mira a proteggere le vittime di violenza domestica, già prevede l'adozione di meccanismi di controllo dell'età sotto la supervisione dell'ARCOM.

La CNIL ha sostenuto la regolamentazione proposta di ARCOM in due ambiti chiave. In primo luogo, ha appoggiato la raccomandazione di utilizzare un verificatore terzo indipendente per garantire la protezione dei dati degli individui. In secondo luogo, ha accolto con favore la previsione di offrire agli utenti internet almeno un sistema di verifica dell'età chiamato "doppio anonimato". Nello specifico, questo sistema garantisce che il sito a cui accede l'utente ottenga la conferma della sua età senza conoscerne l'identità, mentre il fornitore del sistema di verifica dell'età conosce l'identità dell'utente ma non sa a quali siti ha avuto accesso.

Tuttavia, la CNIL ha suggerito all'ARCOM di chiarire il ruolo del terzo verificatore indipendente riguardo ai documenti di verifica dell'età e alla creazione di prove di età riutilizzabili per facilitare la diffusione del sistema a doppia anonimizzazione.

La CNIL ha evidenziato che la verifica dell'età rappresenta solo uno dei vari strumenti disponibili per proteggere i minori online. È fondamentale combinare questa misura con l'uso di sistemi di controllo parentale e, in generale, promuovere un'educazione digitale efficace sia per i giovani sia per gli adulti che li accompagnano, al fine di garantire una maggiore sicurezza su Internet.

La CNIL ha, infine, ribadito che la verifica dell'età dovrebbe essere applicata solo in contesti specifici, soprattutto in situazioni in cui i minori possono trovarsi in pericolo. Una sua applicazione indiscriminata potrebbe infatti portare a un ambiente digitale chiuso, in cui agli utenti viene richiesto costantemente di dimostrare la propria età, o addirittura la propria identità, mettendo a rischio diritti e libertà fondamentali, come quello di espressione.

This document is confidential to Avvera and is subject to copyright protection

AVVERA

SEDE LEGALE E OPERATIVA
20146 MILANO
VIA SARDEGNA, 21

SEDE OPERATIVA CERTIFICATA
21040 ORIGGIO (VA)
LARGO UMBERTO BOCCIONI, 1

ALTRE SEDI
61211 PESARO (PU)
VIA GIASONE DEL MAINO, 13
33100 UDINE (UD)
VIA G. TULLIO, 22

TELEFONO
+39 0296515401

FAX
0296515499

C.F./P.IVA 06047090961
CAP. SOC. 300.000 EURO I.V.
REG. IMPO. MI
06047090961
REA 1866500

WWW.AVVERA.IT
AVVERA@LEGALMAIL.IT

IMQ CERTIFIED
QUALITY MANAGEMENT SYSTEM
ISO 9001:2015

IMQ CERTIFIED
OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEM
ISO 45001:2018

IMQ CERTIFIED
INFORMATION SECURITY MANAGEMENT SYSTEM
ISO/IEC 27001:2013