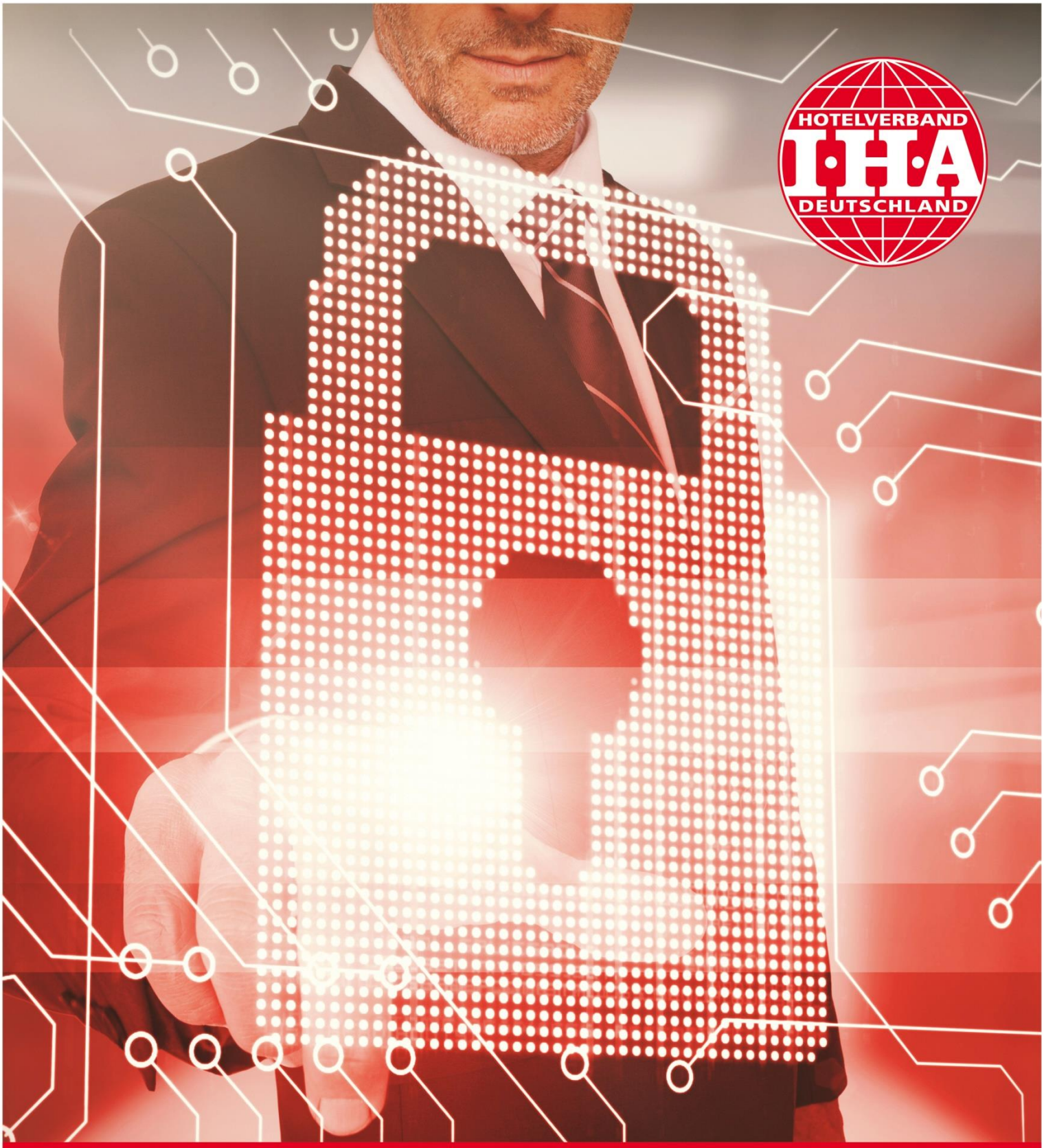

LEITFADEN

DAS NEUE DATENSCHUTZRECHT

INFORMATIONEN & PRAXISTIPPS

GUIDA

LE NUOVE NORME IN MATERIA DI PROTEZIONE DEI DATI

INFORMAZIONI & CONSIGLI PRATICI

ALLEGATO 1 - PANORAMICA DI TUTTE LE LISTE DI CONTROLLO

Lista di controllo relativa a dati riferiti a persone

	Nel vostro albergo esiste la consapevolezza dell'importanza della protezione dei dati e dei relativi rischi?
	In materia di protezione dei dati esistono dei concetti, ad es. direttive interne, documentazioni degli obiettivi, delle responsabilità e dei rischi legati alla protezione dei dati, che possono essere ampliati, se del caso?
	I singoli reparti conoscono i provvedimenti tecnico-organizzativi (PTO) già in essere ai fini della garanzia della protezione dei dati?
	Chi è competente nei singoli reparti per la futura attuazione dei PTO?
	I collaboratori sono addestrati per riconoscere i dati riferiti a persone nell'ambito dell'attività lavorativa quotidiana?
	Dispone ogni reparto di una panoramica delle attività di trattamento legate a dati riferiti a persone?

Lista di controllo per il trattamento di dati

	Analizzate quali tipi di dati riferiti a persone vengono trattati nel vostro albergo? Tra i dati riferiti a persone vi sono delle categorie particolari?
	Vengono mai trattati dati riferiti a persone di bambini?
	Su quale base avviene il trattamento di dati nel vostro albergo?
	Esistono dei set di dati che sono stati trattati sulla base di un consenso non conforme? In passato si sono verificate infrazioni al divieto di abbinamento di dati?
	Il vostro albergo offre una newsletter online? Come sono stati rilevati gli indirizzi e-mail dei destinatari?
	Aggiornate il modulo d'iscrizione alla newsletter? Contiene un riferimento al diritto di revoca?
	Utilizzate il sistema di double opt-in per la registrazione alla newsletter?
	La sottopagina del sito Web che contiene il modulo d'iscrizione è criptata?
	Le CGC da voi utilizzate contengono dei consensi al trattamento dei dati? Se sì, l'indicazione relativa al consenso è facilmente percepibile?
	Le disposizioni in materia di protezione dei dati contengono un riferimento esplicito al diritto di revoca?
	Sul sito Web, il vostro albergo ottempera all'obbligo di informazione in materia di trattamento di dati riferiti a persone? Aggiornate le disposizioni in materia di protezione dei dati?

Lista di controllo per l'esecuzione del mandato

	Incaricate esterni quali incaricati del trattamento di dati riferiti a persone?
	Su quale base gli incaricati del trattamento intraprendono l'attività per voi?
	I contratti con incaricati del trattamento sono stati aggiornati in relazione alle direttive in materia di protezione dei dati e contengono gli stessi indicazioni minime giusta l'art. 28 cpv. 3 RGPD?
	Finora, l'incaricato del trattamento ha fornito la garanzia di una gestione confidenziale dei dati riferiti a persone a lui trasmessi?
	Interpellate i vostri incaricati del trattamento di dati riferiti a persone in merito al nuovo regolamento in materia di protezione dei dati personali e richiedete una conferma scritta attestante che essi seguono una formazione in materia.
	D'ora in poi documentate le direttive che rilasciate all'indirizzo degli incaricati del trattamento.
	Con tutti gli altri vostri contraenti stipulate degli accordi aggiuntivi atti a garantire che il trattamento di dati riferiti a persone sia conforme alla protezione dei dati.

Lista di controllo riguardo al responsabile della protezione dei dati

	Il vostro albergo dispone di un responsabile della protezione dei dati? Se no, perché no? Documentate i motivi delle vostre considerazioni.
	Nel vostro albergo vengono trattati dati sensibili riferiti a persone di particolari categorie? Oppure almeno dieci collaboratori sono costantemente incaricati del trattamento di dati riferiti a persone? In tal caso è d'obbligo nominare un responsabile della protezione dei dati.
	Se invece il vostro albergo non necessita di un responsabile della protezione dei dati, chi nella vostra azienda è competente per il monitoraggio del rispetto della protezione dei dati?
	Se, entro breve, nominerete un responsabile della protezione dei dati: valutate gli argomenti che depongono contro la nomina di un responsabile aziendale della protezione dei dati.
	Un responsabile aziendale della protezione dei dati è certificato come tale? In caso contrario, di quale altra qualifica dispone?
	Il nominativo del responsabile della protezione dei dati è stato notificato all'autorità di vigilanza?
	I collaboratori sono stati adeguatamente formati e sanno quando devono coinvolgere il responsabile della protezione dei dati?
	Il responsabile della protezione dei dati provvede a una formazione annuale dei collaboratori?
	In quali intervalli il responsabile della protezione dei dati informa la direzione sulla sua attività?
	La collaborazione con il responsabile della protezione dei dati viene documentata?

Lista di controllo dell'attività di trattamento e valutazione dell'impatto sulla protezione dei dati

	Esiste già un registro delle attività di trattamento? In caso affermativo, controllate se i requisiti dell'art. 30 RGPD possono eventualmente essere estesi.
	Per il vostro albergo sussiste l'obbligo di tenere un registro? In caso contrario, come si ottempera all'obbligo di documentazione che sussiste comunque?
	Chi in azienda è competente per la tenuta e per l'aggiornamento del registro?
	Il registro contiene tutte le indicazioni obbligatorie?
	Nel registro vengono incluse anche indicazioni facoltative? In caso contrario, con quali mezzi alternativi avviene la documentazione?
	È stata eseguita una valutazione dei rischi? Il risultato è stato documentato?
	In base al risultato della valutazione dei rischi, sussiste l'obbligo della valutazione d'impatto sulla protezione dei dati?
	Chi è competente per l'esecuzione della valutazione dell'impatto sulla protezione dei dati?
	Esistono provvedimenti tecnico-organizzativi (PTO) che, pur non ancora presi, sono accettabili per ridurre ulteriormente i rischi legati ai dati trattati?
	È possibile configurare le impostazioni tecniche di base delle apparecchiature e dei software onde limitare la diffusione di dati riferiti a persone („privacy by default“)?

Lista di controllo della sicurezza delle pagine Web dell’hotel e della rete WLAN dell’hotel?

	In azienda o presso una ditta esterna, i collaboratori dispongono di un interlocutore che li consiglia in materia di sicurezza IT?
	I software delle apparecchiature dei collaboratori, ossia portatili, tablet, smartphone ecc., sono aggiornati?
	Tutti gli apparecchi vengono regolarmente controllati con uno scanner anti-malware?
	Le reti WLAN dei collaboratori e degli ospiti d’albergo sono separate?
	Sul sito Web dell’albergo vengono creati regolarmente dei profili utenti? Si dispone del consenso degli interessati?
	Sono criptate tutte le sottopagine del sito Web che contengono moduli d’iscrizione per l’inserimento di dati riferiti a persone?
	I collaboratori conoscono l'importanza degli avvertimenti dei browser in caso di problemi SSL (siti Internet non criptati)?
	La rete WLAN è protetta da password? Le password standard vengono cambiate regolarmente?
	La password viene generata mediante dati riferiti a persone? In caso affermativo, perché è necessario? È richiesta la documentazione nel registro delle attività di trattamento.
	Le disposizioni in materia di protezione dei dati (ivi compresi gli obblighi d’informazione) della pagina Web sono aggiornate?
	Le disposizioni in materia di protezione dei dati e le condizioni di utilizzo per gli accessi alla WLAN sono aggiornate?

Lista di controllo riguardo alla trasmissione di dati a terzi

	Vengono trasmessi dati a terzi al di fuori dell'UE? In proposito si ricorre alla consulenza di uno specialista?
	In caso affermativo, il destinatario dei dati dispone di un rappresentante della protezione dei dati? I dati di contatto di questa persona figurano nel registro delle attività di trattamento.
	Se dati vengono trasmessi a terzi all'interno o al di fuori dell'UE, qual è la base giuridica che consente la trasmissione?
	La base giuridica è citata nel registro delle attività di trattamento?
	Vengono trasmessi dati a reparti centralizzati all'interno di un gruppo? I nominativi degli interlocutori nei reparti destinatari di questi dati figurano nel registro delle attività di trattamento?

Lista di controllo riguardo al diritto di informazione e di accesso ai dati personali

	Le condizioni di protezione dei dati sul sito Web dell'albergo sono aggiornate? Le condizioni di protezione dei dati sono accessibili da ogni sottopagina del sito Web?
	Il sito Web e i documenti contrattuali ottemperano al diritto degli interessati di essere informati preventivamente sui dati riferiti a persone che vengono trattati e a quale scopo?
	Nei contratti e sul sito Web, si informa gli interessati in modo chiaro sul diritto di informazione, di opposizione e di cancellazione?
	Nelle disposizioni in materia di protezione dei dati il responsabile della protezione dei dati è citato come interlocutore?
	Chi in albergo è competente per rispondere ad eventuali domande circa il trattamento di dati e per gestire l'eventuale opposizione al trattamento di dati?
	Sul sito Web figura il nominativo dell'interlocutore che può fornire informazioni su dati riferiti a persone già trattati (diritto all'informazione a posteriori)?
	Il collaboratore incaricato è adeguatamente formato e sa quali dati possono essere trasmessi e in quali circostanze?
	Esistono guide standardizzate che consentono di rispondere in modo rapido e completo alle richieste degli interessati?
	I collaboratori che trattano regolarmente dati riferiti a persone conoscono il nome di un interlocutore presso l'autorità di vigilanza?
	È garantito che, in caso di richiesta, all'autorità di vigilanza possa essere trasmesso subito il registro delle attività di trattamento oppure un altro tipo di documentazione?

Lista di controllo riguardo alla cancellazione di dati

	Per tutte le categorie di dati sono documentati, con ripresentazione regolare, i periodi di conservazione e di cancellazione (a dipendenza delle finalità del rispettivo trattamento)?
	Esiste una direttiva interna (concetto di cancellazione) che stabilisce il periodo di cancellazione di dati una volta che lo scopo della relativa raccolta viene meno?
	Le competenze della procedura di cancellazione sono regolamentate?
	In caso di opposizione dell'interessato all'utilizzo dei dati, come vengono attuati i divieti di raccolta nella banca dati?
	Quando un interessato chiede la cancellazione dei dati che lo riguardano e se gli stessi sono precedentemente stati trasmessi a terzi, esiste una procedura che prevede che il responsabile informi anche questi uffici affinché i dati vengano cancellati?

Lista di controllo riguardo alla gestione delle violazioni della protezione dei dati

	A chi in albergo compete notificare le violazioni della protezione dei dati all'autorità di vigilanza?
	È garantito che la notifica avvenga entro 72 ore dalla presa d'atto della violazione dei dati?
	In albergo è stato appurato in quali ambiti del trattamento di dati sussiste un rischio elevato di violazioni della protezione dei dati?
	In albergo sono state prese misure efficaci per identificare le violazioni dei dati il più presto possibile?
	I collaboratori sono adeguatamente formati e sanno come comportarsi in caso di violazione della protezione dei dati?

Lista di controllo riguardo alla protezione dei lavoratori

	Quali dati riferiti a persone di categorie particolari di lavoratori e candidati vengono trattati?
	È garantita una protezione speciale per categorie particolari di dati personali?
	Su quale base legale vengono trattati dati di lavoratori? I lavoratori hanno rilasciato un consenso scritto conforme alla legge?
	Gli accordi aziendali in materia di protezione dei dati sono aggiornati?
	Come vengono custoditi i documenti contenenti dati dei lavoratori e dei candidati?
	Chi ha attualmente accesso ai dati dei lavoratori e dei candidati? È possibile provvedere ad una regolamentazione più restrittiva?
	Quali misure vengono attuate per fa sì che le documentazioni di candidatura inoltrate online godano almeno della stessa protezione di quelle cartacee? Esiste una protezione di accesso adeguata?
	La sottopagina che consente l'inoltro online di candidature è criptata?
	I candidati che inoltrano una candidatura online vengono informati sul tipo e l'entità di trattamento dei loro dati? Le condizioni di protezione dei dati sono aggiornate in tal senso?
	I collaboratori sono adeguatamente formati riguarda al diritto d'accesso, di opposizione e di cancellazione dei lavoratori e dei candidati?
	La cancellazione dei dati di candidati e dei lavoratori che hanno lasciato l'albergo è regolamentata?
	I periodi di cancellazione sono documentati nel registro delle attività di trattamento?
	L'accordo sull'elaborazione dei dati è stato controllato da una piattaforma di e-recruiting?
	Il comitato d'azienda è informato sulle novità in materia di protezione dei dati?