Am 25. Mai 2018 tritt die Datenschutz-Grundverordnung *DSGVO* (General Data Protection Regulations - GDPR) in Kraft - eine EU-weite Verordnung und Regelung zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen.

Zur Erfüllung der DSGVO ist eine umfangreiche Regulierung von Geschäftsprozessen, Verträgen, internen Aufzeichnungen, Datenschutzrichtlinien und Softwarenutzung erforderlich. Einen ausführlichen Überblick erhalten Sie hier:

Wie hoch sind 4% Ihres weltweiten Jahresumsatzes? Sind das mehr als 20 Mio. EUR, ist die maximale behördliche Bußgeldhöhe auf diesen Betrag gedeckelt. Ist es weniger als 20 Mio. EUR beträgt die maximal mögliche behördliche Bußgeldhöhe ebenfalls 20 Mio. EUR. Im Falle nicht DSGVO-konformer Unternehmen sind Datenschutzbehörden (Aufsichtsbehörden) der jeweiligen Mitgliedstaaten dazu berechtigt Bußgelder i.H.v. bis zu 20 Mio. EUR bzw. 4% des weltweiten Jahresumsatzes zu verhängen - wobei jeweils der höhere dieser beiden Werte zugrunde gelegt wird. Diese Bußgeldhöhe ist beispiellos in der bisherigen Gesetzgebung zum Datenschutz.

Es dauert für einen Kunden nur wenige Minuten, eine Aufsichtsbehörde aufzusuchen und eine Beschwerde einzureichen, sollten Sie nicht DSGVO-konform agieren. Es reicht bereits eine einzige Datenschutzverletzung für die Verhängung von Sanktionen. Auch wenn jede Aufsichtsbehörde ihre eigenen Prioritäten bei der Durchsetzung aufstellt, so wird keine die Möglichkeiten ignorieren, mit Bußgeldern auf nicht konforme Unternehmen in risikoreichen Branchen - wie etwa der Hospitality Branche - zu reagieren. Sehen Sie hierzu: http://www.hotelnewsnow.com/articles/50937/Timeline-The-growing-number-of-hotel-data-breaches

Der Hoist Group ist die reibungslose und erfolgreiche Integration der DSGVO für alle angebotenen Leistungen ein sehr wichtiges Anliegen. Datenschutzgesetze sind Menschenrechte und wir sind davon überzeugt, dass die richtige Anwendung des Datenschutzes entscheidend ist! Hoist Group verfolgte die Einführung der Vorgaben bereits vor ihrer Verabschiedung und ist auf den 25. Mai vorbereitet. Hoist Group hat bereits folgende Maßnahmen umgesetzt:

- Hoist Groups High Speed Internetzugang (HSIA - High Speed Internet Access) und Property Management Systems Lösungen (PMS) sind anhand des europäischen Datenschutz-Gütesiegels (European Privacy Seal - IAPP) geprüft und es wurde bereits eine DSGVO Konformität festgestellt bzw.sind die Vorbereitungen dazu getroffen. Unsere PMS - HotSoft Kunden sollten sich hiermit vertraut machen: https://www.hoistgroup.com/sv/nyheterpress/2017/12/22/hotsoft-gdpr-compliance-faq-2/
- Einrichtung von Systemen und Richtlinien für SARs (Subjekt Access Requests)
- Ernennung eines Datenschutzbeauftragten im HQ Stockholm, Schweden
- Erstellung eines Meldeprotokolls sowie ein internes Systemmanagement bei Verstößen
- Mitarbeiterschulungen in Bezug auf SARs & Verstöße (im Falle von Datenschutzverletzungen)
- Zertifiziert, dass der gesamte Datenexport aus der EU im Rahmen von Musterverträgen erfolgt und das sich der Auftragsverarbeiter der betroffenen Daten DSGVO-konform verhält
- Ergänzung jedes Drittanbietervertrags um DSGVO-konforme Bedingungen
- Aktualisierung der Datenschutzerklärung und Bereitstellung von Beispieldatenschutzerklärungen für die Datenverantwortlichen
- Implementierung der „Privacy by Design“ in der Neuproduktentwicklung

Hoist Group ist Ihr verlässlicher Geschäftspartner, wenn Sie DSGVO-konforme Services und Verträge abschließen, von Beginn an einen Datenschutzbeauftragten an Ihrer Seite habe wollen und ein effizientes und realistisches Handeln hinsichtlich der Datensicherheit - von Meldepflichten bis hin zu SARs - voraussetzen. Hotels sind auf die Zuverlässigkeit ihrer Systemanbieter angewiesen. Stellen Sie sicher, dass Ihr Anbieter dazu bereit ist, Sie zu schützen.

Jedes Hotel in der EU unterliegt der Pflicht, …

- eine Verletzung der Datensicherheit zu erkennen und diese seiner Aufsichtsbehörde innerhalb von 72 Stunden nach Entdeckung des Verstoßes zu melden.
- jedem Kunden innerhalb von 30 Tagen eine Kopie seiner gespeicherten Daten zur Verfügung zu stellen und einen Mechanismus für mögliche Anfragen dieser Art anzubieten. Diese Anfragen werden als *Subject Access Requests* (SARs) bezeichnet.
- eine Datenverarbeitung außerhalb der EU einzustellen oder DSGVO konforme Regelungen bzw. andere Schutzmaßnahmen für den Datenexport außerhalb der EU einzurichten.
- jederzeit die DSGVO-Konformität bei seiner zuständigen Aufsichtsbehörde nachweisen zu können.
- alle Service-Provider-Verträge, die relevante Daten entsprechend der DSGVO beinhalten, neu zu formulieren bzw. zu aktualisieren (nahezu in allen Fällen).
- seine Datenschutzrichtlinien zu aktualisieren.
- die Einwilligungserklärung personenbezogener Daten zu aktualisieren, um die tatsächliche Verwendung und Nutzung der betreffenden Daten offenzulegen.
- die rechtliche Grundlage für die Verarbeitung von personenbezogenen Daten zu kennen und
- auf einen Widerruf der Einwilligung und Löschungsanfragen umgehend reagieren zu können.

Im Folgenden finden Sie ein umfassendes Konzept für Ihren Start in die DSGVO-Konformität:

1. Erstellen Sie ein Datenmappe

Welche personenbezogenen Daten liegen Ihnen vor, wo speichern/legen Sie diese Daten ab und wer hat Zugriff auf diese Daten? Sobald Sie sich Klarheit über diese Ausgangssituation verschafft haben, sind Sie in der Lage, strukturiert vorzugehen. Dies schließt auch folgende Daten ein:

- Ihre Mitarbeiterinformationen und all Ihre HR-Daten
- Ihr Property Management System (PMS)
- Alle Schnittstellen und Subsysteme in der Datenweiterleitung,
- die mit Ihrem PMS-System verlinkt sind
- Ihren externen Kundendienst
- Ihr Abrechnungssystem (POS) sowie Ihre PCCI-Punkte
- Ihre Spa-Reservierungen
- Konnektivitäts-Informationen/ Verbindungsinformationen Ihrer Gäste - was befindet sich auf Ihren Routern? Worauf kann man mit Hilfe Ihres TV-Systems zugreifen?
- Metadaten - Ihre Protokolle und Logdateien
- Ihre Service-Tickets, insbesondere Ihre Aufzeichnungen

Wie werden diese Daten verarbeitet? Wo und wie werden sie gespeichert und wer hat Zugriff auf diese Daten? Nutzen Sie Cloud-Services für die Datenverarbeitung und wo befinden sich Ihre Server?

Bewahren Sie all diese Informationen an einem geschützten Ort auf. Dies ist der erste Schritt Ihrer Dokumentation und wird auch als Datenregister oder Datenmappe bezeichnet. Sie müssen jederzeit in der Lage sein, Ihrer Aufsichtsbehörde diese Datenmappe vorweisen können.

2. Wer pflegt die Datenmappe?

In jedem Abschnitt Ihres Datenflusses gibt es Personen, die auf diese Daten zugreifen können. Es muss in einfachen und effizienten Schritten nachvollziehbar sein, dass all diese Personen rechtlich bindende Geheimhaltungsverpflichtungen eingegangen sind - im Rahmen eines Mitarbeitervertrags, eines Subunternehmervertrags oder eines Datenverantwortlichen- /Datenverarbeitungsvertrags.

Die betreffenden Personen müssen über die DSGVO aufgeklärt sein, um im Falle einer Datenschutzverletzung oder einer SAR (Subject Access Request) Ihren Datenmanager oder Datenschutzbeauftragten kontaktieren und diese Informationen weiterleiten zu können.

3. Darf Ihr Datenfluss die EU verlassen?

Es ist möglich, personenbezogene Daten unter Erfüllung der DSGVO-Verordnung aus der EU zu exportieren. Dies erfordert jedoch eine gewisse Sorgfalt, unter Einhaltung von DSGVO konforme Regelungen vor Ort. Unter gewissen Umständen ist auch eine EU-Präsenz des datenempfangenden Vertragspartners nachzuweisen. Die Empfängerpartei der exportierten Daten muss daher ebenfalls DSGVO-konform sein. Werden die exportierten Daten weiter verarbeitet, hat der Datenverantwortliche das Recht auf Prüfung des Datenverarbeitenden. Befindet sich Ihr PMS-System in der Cloud und die Server oder Kundendienstmitarbeiter außerhalb der EU, findet die DSGVO weiterhin Anwendung und es bedarf eines DSGVO-konformen Services.

4. Welche Schutzmaßnahmen müssen Sie treffen?

Personenbezogene Daten, die in ihren Systemen liegen, müssen durch geeignete technische so wie physische Maßnahmen geschützt werden. Dies bedeutet, dass die Möglichkeiten zur Verschlüsselung von Daten genutzt werden soll. Dies hat wiederum zur Folge, dass Datendepots (Repositorien) die personenbezogene Daten enthalten (wie bspw. PMS Systeme) den Zugriff auf eindeutig zuordenbare Accounts protokollieren müssen. Entsprechend haben Sie Ihre Netzwerke durch eine Firewall zu schützen, Zugangstüren unter Verschluss zu halten und betroffene Gebäude angemessen zu sichern. Diese Vorkehrungen sind ebenfalls in das Datenregister bzw. die Datenmappe aufzunehmen und zu protokolieren.

Betriebssysteme wie Outlook oder G-Suites, die Sie in Ihrem Betrieb nutzen, verfügen über eigene Compliance-Verpflichtungen, auf die Sie sich berufen können. Sie müssen jedoch die Kenntnis darüber besitzen, was Sie tatsächlich nutzen und einen entsprechenden Vertrag vorlegen, auf welchen Sie Bezug nehmen können.

5. Was müssen Sie Ihren Kunden mitteilen?

Ihre Datenschutzrichtlinien sind der Maßstab zur Einhaltung der DSGVO. Sie müssen nicht in den Geschäftsbedingungen auf Ihrer Webseite enthalten sein. Jedoch ist eine separate, kurze, klare und direkt an den Kunden gerichtete Erläuterung empfehlenswert, die offenlegt, welche Informationsansprüche bestehen (die Rechtsgrundlage bezüglich der Datenverarbeitung, der gesammelte Datenumfang, die Art der Datennutzung, -aufbewahrung und -verteilung sowie die Löschung der Daten).

Kombinieren Sie dies mit einer Handlungsaufforderung (eine Verlinkung zur Aufsichtsbehörde im Falle einer Beschwerde, eine E-Mail Adresse oder eine Verlinkung zu den SARs).

6. Wann ist eine Einwilligung des Dateninhabers einzuholen?

Jedes Unternehmen, das personenbezogene Daten verwendet, benötigt hierfür eine Rechtsgrundlage. Der Vertrag zur Nutzung personenbezogener Daten stellt die Rechtsgrundlage dar. Um ein Hotelzimmer und die damit verbundenen Dienstleistungen anbieten zu können, benötigt ein Hotel bestimmte Informationen. Diese Art der Informationen bedarf keiner vorherigen Zustimmung. Es bedarf ebenso keiner Einwilligung, wenn das Hotel - und nur ausschließlich das Hotel, nicht die Hotelkette - weiterhin mit dem Gast in Kontakt steht. (Jedoch muss dem Gast jederzeit die Möglichkeit für einen Wiederspruch eingeräumt und zur Verfügung gestellt werden)

Eine Einwilligung ist dann zwingend erforderlich, wenn Sie die personenbezogenen Daten an Datenverantwortliche von Drittanbietern weitergeben möchten. Dies gilt auch, wenn Sie Ihren Gast über Angebote von Schwestergesellschaften und -hotels informieren möchten.

Ihr PMS System sollte über eine Tracking-Funktion hinsichtlich der Einwilligung verfügen. Beabsichtigen Sie eine umfassendere Verwendung der personenbezogenen Daten, müssen Sie sich mit dieser Thematik vertraut machen. Unternehmen und Betriebe müssen in der Lage sein, Ihrer Aufsichtsbehörde (die Regierungsbehörde, die Ihre Datennutzung regelt) eine Einverständniserklärung vorlegen zu können. Diese müssen auf Wunsch des betroffenen Dateninhabers umgehend und jederzeit wiederrufbar sein.

Die Einwilligung zur Datennutzung darf nicht automatisch in der Einwilligung der AGBs enthalten sein. Der Dateninhaber muss seine Zustimmung aktiv (bspw. über das bewusste setzten eines Hackens) abgeben. Hierbei muss der Wortlaut der Einwilligungsanfrage mit dem tatsächlichen Verwendungsgrund/-zweck der Daten übereinstimmen.

7. Benötigen Sie einen Datenschutzbeauftragten (DPO - Data Protection Officer)?

Unter gewissen Umständen benötigen Sie einen Datenschutzbeauftragten - eine interne oder externe Person, die für die Einhaltung der DSGVO in Ihrem Hotel zuständig ist. Wenn Sie Franchisenehmer sind, wurde diese Entscheidung mit großer Wahrscheinlichkeit bereits auf Unternehmensebene getroffen. Zählt Ihr Betrieb zur Privathotellerie, benötigen Sie nicht zwingend einen eigenen Datenschutzbeauftragten – jedoch könnte Ihr PMS- und/oder Internet-Service-Provider hiervon betroffen sein.

8. Wie setzten sich Ihre Verträge zusammen?

Wenn ein Hotel für sein PMS-System einen Cloud-Service für die Datenverarbeitung nutzt, so handelt es sich bei dem Hotel um den Datenverantwortlichen und bei dem PMS-Anbieter um den Datenverarbeiter. Die DSGVO schreibt einen schriftlichen Vertrag vor, der bestimmte Elemente des Datenaustausches ausdrücklich regelt.

Nimmt ein Hotel die Dienstleistung eines PMS-Anbieters außerhalb der EU in Anspruch, ist es zwingend notwendig diesen Datenexport anhand von Musterverträgen fehlerfrei und vollständig zu dokumentieren und nachzuverfolgen.

In der Rolle der Datenverantwortlichen haben Hoteliers das Recht, ihre Datenverarbeiter um Unterstützung bei der Bearbeitung der SARs zu bitten - befinden sich Ihre Datenverarbeiter auf dem aktuellsten Stand? Sind Sie darüber informiert, wer Datenschutzbeauftragte Ihrer Datenverarbeiter ist?

Ihre Verträge müssen folgende Punkte beinhalten und beantworten: wer ist Datenverarbeiter und wer ist Datenverantwortlicher, welche Daten sind betroffen, welcher Rechtsgrundlage unterliegt die Verarbeitung, welche Prüfrechte besitzt der Datenverantwortliche, das Recht auf Kenntnis des Datenverantwortlichen über alle Schnittstellen und Subsystemen für die Datenverarbeitung, die Richtlinien zur Datenlöschung durch den Datenverantwortlichen, sowie jegliche Unterstützungsmaßnahmen, die vom Datenverarbeitenden im Falle einer Datenverletzung oder SARs angeboten werden.

9. SARs (Subject Access Requests) - Zugriffsanfragen

Ab Mai 2018 haben betroffene Personen das Recht auf den Zugriff, die Löschung und die Änderung ihrer personenbezogenen Daten. Jede Person, die Ihre Dienstleistungen und Services jemals in Anspruch genommen hat, kann Sie schriftlich - elektronisch oder postalisch - um die Aushändigung einer Kopie aller Ihnen vorliegenden, personenbezogenen Daten bitten. All diese personenbezogenen Daten können äußerst umfassend ausfallen: dazu gehören Metadaten, ihre MAC-Adressen, aber auch vom Kundendienst erfasste Telefonnummern in einem Support-Ticket. Selbiges gilt für Rechnungen und Barbelege.

Diese Art der Anfrage, die eine Person zur Aushändigung ihrer personenbezogenen Daten stellt, wird als sogenannte Subject Access Request (SAR) bezeichnet. SARs sind an den Datenschutzbeauftragten weiterzuleiten und zu protokolieren. Eine Rückmeldung auf eine SAR hat innerhalb von 30 Tagen zu erfolgen. Jedes Hotel benötigt eine unmissverständliche Datenschutzbestimmung, mit einer klaren und einfachen Kontaktmöglichkeit für SARs – auch wenn bestimmte Anfragen aufgrund ihrer Art (Sinnhaftigkeit) keinen Handlungsbedarf erfordern. Aber unverändert gilt: Wenn Sie in Ihrem EU-Mitgliedsland bspw. einer Aufbewahrungspflicht für Rechnungen unterliegen, müssen Sie eine betreffende Rechnung nicht vernichten, nur weil Sie eine personenbezogene Informationen enthält.

10. Das Verstoß- bzw. das Verletzungsprotokoll

Im Falle einer Datenverletzung müssen Ihr Hotel und Datenverarbeiter in der Lage sein, diesen Verstoß zu erkennen, zu untersuchen und im Bedarfsfall zu melden. Dies bezieht sich sowohl auf den Umfang der Verletzung, die Reaktionsgeschwindigkeit und die Vollständigkeit. Prüfen und klären Sie daher folgende Aussagen in Ihrem Betrieb: sind Ihre Datenverarbeiter qualifiziert, einen Verstoß zu erkennen und welchen Weg der Kontaktaufnahme würden sie im Falle eines Verstoßes wählen, um Sie in Kenntnis darüber zu setzten? Auf welche Art kontaktieren Sie Ihre Kunden? Sind alle Beteiligten innerhalb der Informationskette über die vorgegebene 72-Stunden Reaktionsfrist informiert?

11. Wann findet Ihr Training statt?

Die Schulung Ihrer Mitarbeiter und Datenverarbeiter hinsichtlich der SAR-Anfragen und des Verstoß- bzw. Verletzungsprotokolls, erhöhen die Sicherheit der Nachweisführung und die Reaktionsgeschwindigkeiten. Im Falle einer Datenschutzverletzung und Bußgelderhebung könnte dies bei der für Sie zuständigen Aufsichtsbehörde als mildernder Umstand berücksichtigt werden!

12. HR - Human Resources

Bei Ihren eigenen Mitarbeitern handelt es sich ebenfalls um Dateninhaber, dessen hinterlegte bzw. gespeicherte Daten die Definition personenbezogener Daten erfüllen. Daher gilt es, folgende Fragen innerhalb Ihres Betriebs zur Einhaltung der DSGVO zu klären: in welcher Art und Weise werden diese personenbezogenen Daten aufbewahrt und ist ihre Sicherheit vor unbefugtem Zugriff gewährleistet? Sind Sie auf Anfragen Ihrer Mitarbeiter in der Lage Auskunft (in Form einer Kopie) über ihre personenbezogenen Daten zu geben? Haben Sie eine Möglichkeit der zentralen und vollumfänglichen Ablage dieser Daten geschaffen und sichergestellt?

Berücksichtigen Sie ebenfalls personenbezogene Daten abgewiesener Bewerber sowie deren Anfrage nach einer entsprechenden Auskunft. Wie lange verbleiben diese Daten in Ihrem Betrieb und zu welchem Zeitpunkt werden diese gelöscht?

Haftungsausschluss

Die hier dargestellten Inhalte, Standpunkte und/oder vertretenen Ansichten hinsichtlich der DSGVO, in Bezug auf die Hotellerie sowie Hoist Groups Lösungen und Produkte, spiegeln ausschließlich die Meinung der Hoist Group wieder. Im Sinne der Transparenz und Kommunikation zwischen Datenverarbeiter und Datenverantwortlichen, was die DSGVO ausdrücklich unterstreicht, sieht sich Hoist Group in der Pflicht diese Informationen mit Ihnen - unseren Kunden - zu teilen. Hoist Group sieht sich jedoch nicht in der Lage rechtliche Auskünfte über die Umsetzung und Einhaltung der DSGVO zu geben. Daher dienen alle hier bereitgestellten Informationen lediglich zu Informationszwecken. Hoist Group übernimmt in Folge dessen keine Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Die Verantwortung für die Umsetzung und Einhaltung der DSGVO liegt demgemäß bei jedem einzelnen Betrieb/Unternehmen der EU selbst.