PassportScan®

# IL CHECK-IN FACILE
# SCANSIONE, FIRMA ED INVIO

## GDPR COMPLIANT

# PassportScan® / COS'È IL GDPR?

## COS'È IL GDPR?

**Il GDPR è una normativa pensata per dare a chiunque un maggiore controllo dei propri dati.** L'obiettivo che si prefigge è semplificare dei contesti legali complessi, affinché i cittadini e le aziende possano beneficiare pienamente e in maniera trasparente dell'economia digitale.

Effettivamente, quasi ogni aspetto della nostra vita ruota attorno ai dati. Basta pensare a cosa ci richiedono i social media, le banche, i negozi e perfino il governo. Quasi tutti i servizi che utilizziamo comprendono la raccolta e l'analisi dei nostri dati personali. Nome, indirizzo, numero di carta di credito, ecc. vengono difatto raccolti, analizzati e, cosa più importante, immagazzinati dalle organizzazioni.

## COS'È IL GDPR COMPLIANCE?

Secondo i termini del GDPR, **le organizzazioni non solo dovranno garantire che i dati personali siano raccolti legalmente e rigorosamente, ma perfino gli incaricati di tale raccolta saranno obbligati a proteggere i dati dall'uso improprio e dallo sfruttamento, rispettando così i diritti dei proprietari** o andando incontro a pesanti sanzioni, in caso di un mancato rispetto dalla normativa.

## A CHI SI RIVOLGE IL GDPR?

Il GDPR si applica **a qualsiasi organizzazione che opera all'interno dell'UE e a qualsiasi organizzazione fuori dell'UE che offre beni/ servizi a clienti/aziende dell'UE**. Ciò significa che quasi tutte le grandi aziende del mondo dovranno essere pronte e conformi quando il GDPR entrerà in vigore.

La legislazione GDPR dovrà essere applicata da due diversi gestori di dati: iil "**titolare del trattamento**" ed il "**responsabile del trattamento**". Le definizioni di ciascuno sono stabilite nell'articolo 4 del regolamento generale sulla protezione dati.

Un **titolare del trattamento** è "**la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali**", mentre il **responsabile del trattamento** è "**la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del titolare del trattamento**".

Il GDPR obbliga legalmente ad un **incaricato del trattamento** ad un certo tipo di conservazione e registrazione dei dati personali,  fornendo un livello molto più elevato di responsabilità legale, in caso di violazione della normativa.

I **titolari del trattamento** saranno inoltre obbligati a garantire che tutti i contratti con i responsabili del trattamento siano conformi al GDPR.

# PassportScan® / COS'È IL GDPR?

## GDPR, COSA SI INTENDE PER DATI PERSONALI?

I tipi di dati considerati personali, ai sensi della legislazione esistente, sono quelli che includono nome, indirizzo e foto. **Il GDPR estenderà l'attuale definizione dei dati personali in modo che, perfino un indirizzo IP, debba essere visto come un dato personale.** La normativa includerà altri dati personali sensibili, quali dati genetici e dati biometrici, che saranno elaborati al fine d'identificare un individuo in modo univoco.

## QUANDO ENTRA IN VIGORE IL GDPR?

**Il GDPR dovrà essere applicato in tutta l'Unione europea dal 25 maggio 2018** e tutti i paesi membri dovranno trasferirlo nella propria legislazione nazionale entro il 6 maggio 2018.

Dopo quattro anni di preparazione e dopo vari dibattiti, il GDPR è stato approvato dal Parlamento europeo nell'aprile 2016. I testi ufficiali ed il regolamento della direttiva sono stati pubblicati in tutte le lingue ufficiali dell'UE nel maggio 2016.

## QUANDO È IL TERMINE PER IL GDPR COMPLIANCE?

A partire dal **25 maggio 2018** tutte le organizzazioni dovrebbero essere conformi al GDPR.

## GDPR: COSA CAMBIA PER LE IMPRESE?

**Il GDPR stabilirà un'unica legge per tutto il continente ed un insieme di regole per le aziende extraeuropee che comunque tratteranno con l'UE.** Ciò significa che la portata della legislazione si estenderà oltre i confini dell'Europa stessa, perfino alle società con sede al di fuori del nostro continente, ma con attività sul territorio europeo, le quali saranno obbligate al rispetto della normativa GDPR.

La normativa GDPR sarà volta a garantire che la sicurezza sulla protezione dei dati sia incorporata in tutti i servizi e prodotti, sin dalle prime fasi di sviluppo, fornendo la garanzia "**privacy by design**" in qualsiasi nuovo prodotto e tecnologia.

Le organizzazioni saranno anche incoraggiate ad adottare tecniche come la "**pseudonimizzazione**", per trarre vantaggio dalla raccolta e dall'analisi dei dati, mentre la privacy dei clienti dovrà sempre essere rigorosamente protetta.

# PassportScan® / COS'È IL GDPR?

## COS'È IL DATA BREACH?

Quando il GDPR entrerà in vigore, introdurrà l'obbligo per tutte le organizzazioni di segnalare certi tipi di violazione dei dati (come l'accesso non autorizzato o la perdita dati) ad una o più figure responsabili, designate per detto controllo. In alcuni casi, le organizzazioni dovranno perfino informare le persone colpite dalla violazione.

**Le organizzazioni saranno obbligate a segnalare eventuali violazioni che comportano un rischio sui diritti e le libertà delle persone e che possano condurre a discriminazione, danni alla reputazione, perdita finanziaria, perdita di riservatezza o qualsiasi altro svantaggio economico o sociale.**

In altre parole, se verrà violato il nome, l'indirizzo, i dati di nascita, i dati sanitari, i dati bancari o eventuali dati personali dei clienti, l'organizzazione sarà obbligata a comunicarsi con gli interessati e con l'ente normativo competente, in modo che tutto il possibile possa essere fatto per limitare il danno.

Questo dovrà essere fatto **tramite una notifica di violazione**, la quale dovrà essere consegnata direttamente alle vittime. Queste informazioni non potranno essere comunicate viastampa, sui social media e sul sito web aziendale. Si trattera di una corrispondenza personale, diretta con le persone colpite.

La violazione dovrà essere segnalata all'organo di vigilanza competente **entro 72 ore**. Durante questo lasso di tempo, nel caso di una violazione abbastanza seria, la legislazione GDPR sottolinea che i clienti dovranno essere resi partecipi della notizia senza "indebiti ritardi".

## GDPR: SANZIONI

**Il mancato rispetto del GDPR può portare ad una multa che va dai 10 milioni di euro al 4% del fatturato globale annuo della società**, cifra che per alcuni coincide con vari miliardi.
Le multe dipenderanno dalla gravità dell'infrazione e dal non rispetto, da parte della società, delle norme di conformità e sicurezza.

La multa massima è di 20 milioni di euro o del 4% del fatturato globale. Tale importo sarà maggiore in caso di infrazioni dei diritti delle parti interessate, trasferimento di dati personali internazionali ad organizzazioni non autorizzate. Inoltre la non implementazione delle procedure o l'ignorare le richieste di accesso dei soggetti ai loro dati porterà a gravi multe.

Una multa inferiore a 10 milioni di euro o al 2% del fatturato globale verrà applicata alle aziende che gestiscono in modo errato i dati. Rientrano in questi casi, ad esempio, il non segnalare una violazione dei dati, il non creare privacy nel design, il non assicurare che la protezione dei dati sia applicata nella prima fase di un progetto e il non essere conforme con la nomina di un certo responsabile per la protezione dei dati, se il GDPR ritiene che sia utile ad una certa organizzazione.

# PassportScan® / GDPR & PASSPORTSCAN

## LA PROTEZIONE DEI DATI PERSONALI COME DIRITTO FONDAMENTALE

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che **ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano**.

## PASSPORTSCAN MISSION

La missione di **PassportScan** è quella di aiutare gli hotel, di qualsiasi dimensione, **a migliorare la procedura di check-in, ottenendo i dati personali in modo sicuro e trasparente**. I flussi di lavoro presso la reception saranno così ottimizzati, garantendo sempre una corretta e sicura gestione della privacy.

# PassportScan® / PRINCIPI TRATTAMENTO DATI

1.- Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto.

2.- Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati.

3.- Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

4.- Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.

5.- È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.

6.- In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali.

7.- I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento.

8.- Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario.

9.- I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi.

10.- Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica.

11.- È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati.

12.- I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

# PassportScan® / COME TI PUO AIUTARE PASSPORTSCAN?

## CANCELLAZIONE PERIODICA DEI DATI, IN BASE AL CONSENSO

*Onde **assicurare che i dati personali non siano conservati più a lungo del necessario**, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica.*

**PassportScan può essere facilmente configurato dal titolare/responsabile del trattamento per eliminare automaticamente i dati acquisiti in un determinato intervallo di tempo**. Con la finalità di garantire che i dati personali non siano conservati più a lungo del necessario, i limiti di tempo dovrebbero essere stabiliti dal responsabile del trattamento per una certa cancellazione o per una revisione periodica.
Una volta acquisita, l'immagine dell'ID e altri dati sensibili potranno essere oscurati o pixelati in **PassportScan**.
Inoltre, qualsiasi richiesta esplicita di cancellare completamente i dati del cliente comporterà la cancellazione totale dei dati/immagini del cliente in **PassportScan**.

## CONDIZIONI PER IL CONSENSO

***Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano**, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.*

**Il titolare del trattamento, in PassportScan, può aggiungere un massimo di quattro testi che l'ospite può accettare/negare, spuntando una casella sul tablet e firmando.** Normalmente due dei testi sono obbligatori - richiesti dalla legge/istituzioni locali - e il resto può includere qualsiasi tipo di politica non specificamente correlata alla privacy (ad esempio: il fumare in camera, il noleggio bici ecc.).
**PassporScan** offre anche l'opzione di impostare un consenso automatico (la cosiddetta firma zero) che il cliente può leggere e accettare implicitamente al check-in in hotel.
Tutto il testo può essere completamente personalizzato in base alle esigenze specifiche dell'hotel sulla privacy. I testi possono essere caricati in due lingue (normalmente la lingua del paese come lingua principale e l'inglese come seconda).

# PassportScan® / COME TI PUO AIUTARE PASSPORTSCAN?

## DIRITTO ALL'OBLIO

*È opportuno prevedere modalità volte ad **agevolare l'esercizio, da parte dell'interessato**, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, **ottenere** gratuitamente, **in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione**. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.*

Utilizzando **PassportScan**, al momento della firma sul tablet, l'ospite può scegliere di negare/non firmare la politica che richiede di elaborare/mantenere i propri dati personali. **Una negazione di questa politica porterà a una cancellazione totale dei suoi dati.**

## TRATTAMENTO DATI SENSIBILI PRIVACY

***Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura.** Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.*

**PassportScan garantisce un elevato livello di sicurezza, proteggendo tutti i dati acquisiti tramite crittografia** avanzata (Blowfish +) in un unico database condiviso o locale. Tutti i dati sensibili (dati dei clienti, immagini dei documenti e firma biometrica) vengono salvati in un database MySQL Oracle e protetti da crittografia 'BlowFish' a 256 bit.

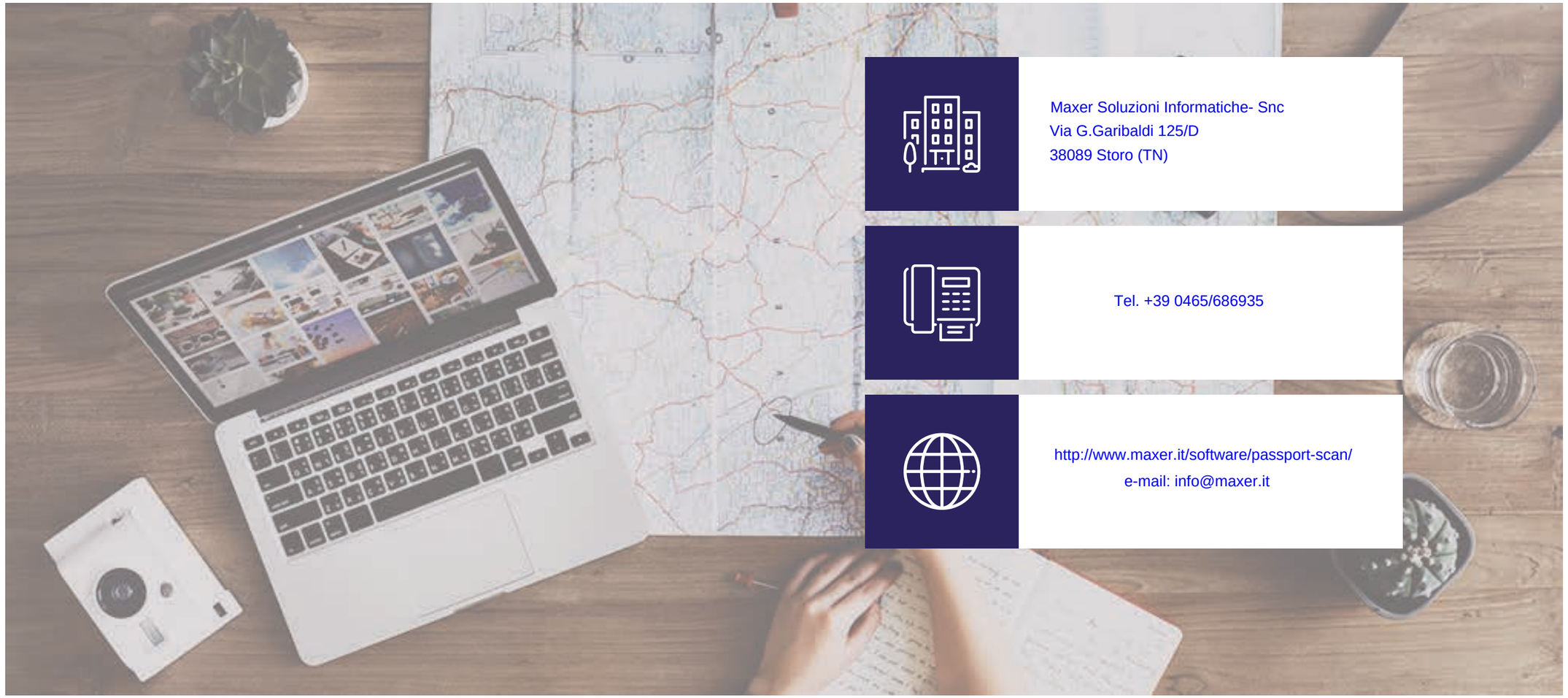
# PassportScan® / COME TI PUO AIUTARE PASSPORTSCAN?

## ASSEGNAZIONE DELLE RESPONSABILITÀ

***La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento****, anche in relazione al monitoraggio e alle misure delle autorità di controllo,* ***esigono una chiara ripartizione delle responsabilità*** *ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.*

**PassportScan offre diversi livelli di accesso basati sulla responsabilità in una determinata organizzazione.** Gli accessi utilizzati sono: User, Superuser e Admin (questi potrebbero essere, ad esempio, in un hotel, rispettivamente per un addetto alla reception, un FOM e un GM/IT).
In questo modo, questa operazione limita l'accesso ai certi dati sensibili agli utenti normali ed evita una minaccia alla sicurezza purtroppo abbastanza diffusa.
Tutte le password utilizzate dai diversi utenti, col GDPR, sono state migliorate in **PassportScan**, in quanto vien ora imposto l'obbligo di creare una password utilizzando lettere maiuscole e minuscole, numeri e caratteri speciali.
Una particolare azione, modifica o processo eseguito da un certo utente, può essere facilmente monitorato con il registro dello storico (**audit)**, altro servizio implementato da **PassportScan** per la conformità col GDPR.

# PassportScan® / CONTATTO




Maxer Soluzioni Informatiche- Snc
Via G.Garibaldi 125/D
38089 Storo (TN)

Tel. +39 0465/686935

http://www.maxer.it/software/passport-scan/
e-mail: info@maxer.it