



**Business  
case**



# Collecting passport information from visitors

## Introduction

The need for collection of visitor passport information is mandatory and regulated within many jurisdictions globally. Therefore, a crucial requirement for most hotels, cruise lines and other accommodation providers.

In most cases, the process for collecting passport information is completely manual and involves copy machines, physical papers and physical archives.

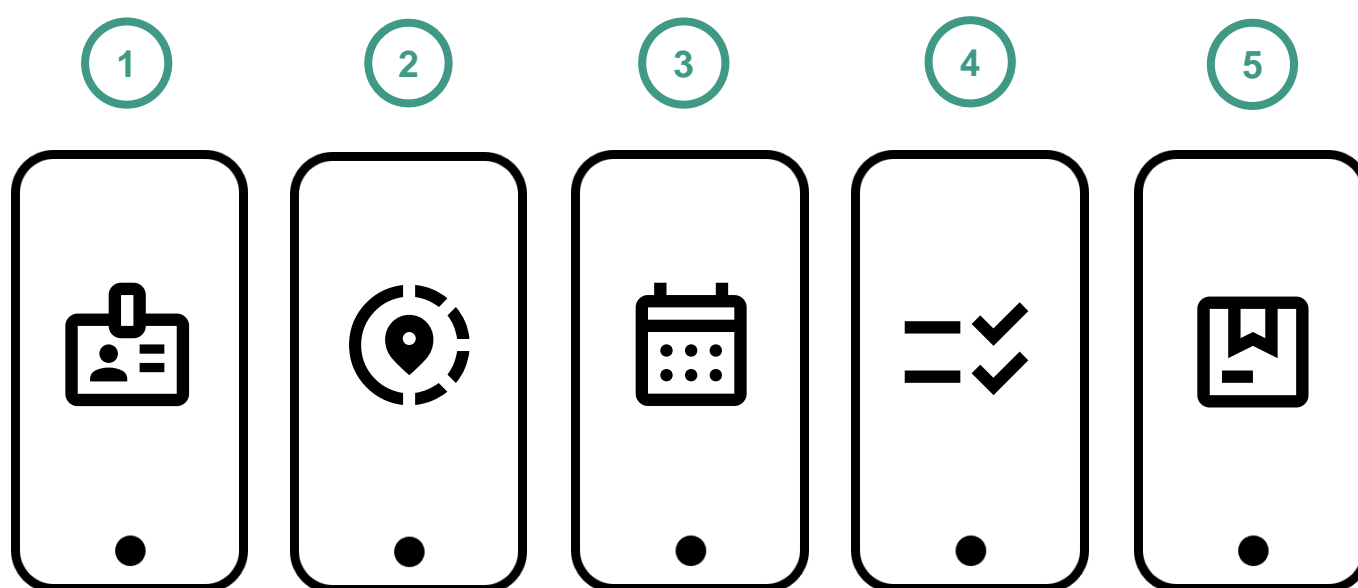
As the passport information per definition is personal information, the handling and involved processes must comply to General Data Protection Regulation (GDPR), Know Your Customer (KYC) and more.

Within many local jurisdictions the passport information is also connected to the reporting of visitors' tax.

## Principles of the solution

We offer a solution based on the Lequinox<sup>®</sup> Distributed Ledger Technology (DLT) that will simplify, secure and streamline all costly and manual processes that collect passport information.

The solution can be offered as a stand-alone solution (using a mobile phone/tablet) or integrated in existing management systems, all in compliance with local and national legislation, including GDPR, KYC and more.



1. Take one or more passport photos for the specific booking.
2. GPS information is stored.
3. Enter arrival and departure date in the calendar.
4. Enter additional information, booking reference, room number and more.
5. Sign and Seal the collected passport information.



**Hewlett Packard  
Enterprise**

a Partner Ready service

- The *Signed and Sealed* passport information is automatically *encrypted, protected and stored* in an own digital archive, including the *irrefutable audit trail* (who did what and when).
- The passport information is *automatically distributed* to the visitor and local government in an encrypted and protected format, if applicable.
- The passport information is *automatically deleted* after a certain time, according to local and national legislation, GDPR, KYC, and more. The visitor is informed when the passport information is deleted.

## Improved visitors experience

During the collection of passport information, the visitor can, if applicable, have an exact copy of the collected information.

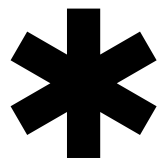
This includes information of deletion of specific passport information and a follow up mail confirming the deletion of passport information and the connected email address.



**Hewlett Packard  
Enterprise**

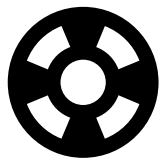
a Partner Ready service

## Your business outcomes



### Risk

- Reduced risk in operations through enforcement of set policies in compliance to local jurisdiction, GDPR, KYC, and more.
- The Lequinox DLT platform ensures that all information is encrypted and protected with an irrefutable audit trail.



### Safety

- Improved safety for both staff and visitors, due to the simplified and streamlined process, including notification of collected passport information and confirmation of deletion.
- The Lequinox DLT platform executes set policies, such as automatic deletion and notification of passport data and more.



### Efficiency

- Extremely fast and lightweight deployment (stand-alone solution as a service). Improved efficiency and saved time in the process of collecting passport information.
- The Lequinox DLT platform ensures that all information is protected in an own digital archive.



### Community

- Improved work environment and dialogue with visitors.
- The Lequinox DLT platform ensures distribution of passport information to visitors and local government in an encrypted and protected format.



### Environment

- Improved environmental footprint, by not printing records and storing them in a physical archive.
- The Lequinox DLT platform creates the foundations to optimise existing or create new processes and services in compliance with regulations.



  
**Hewlett Packard  
Enterprise**

a Partner Ready service