ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals

GDPR & PCI challenges and solutions

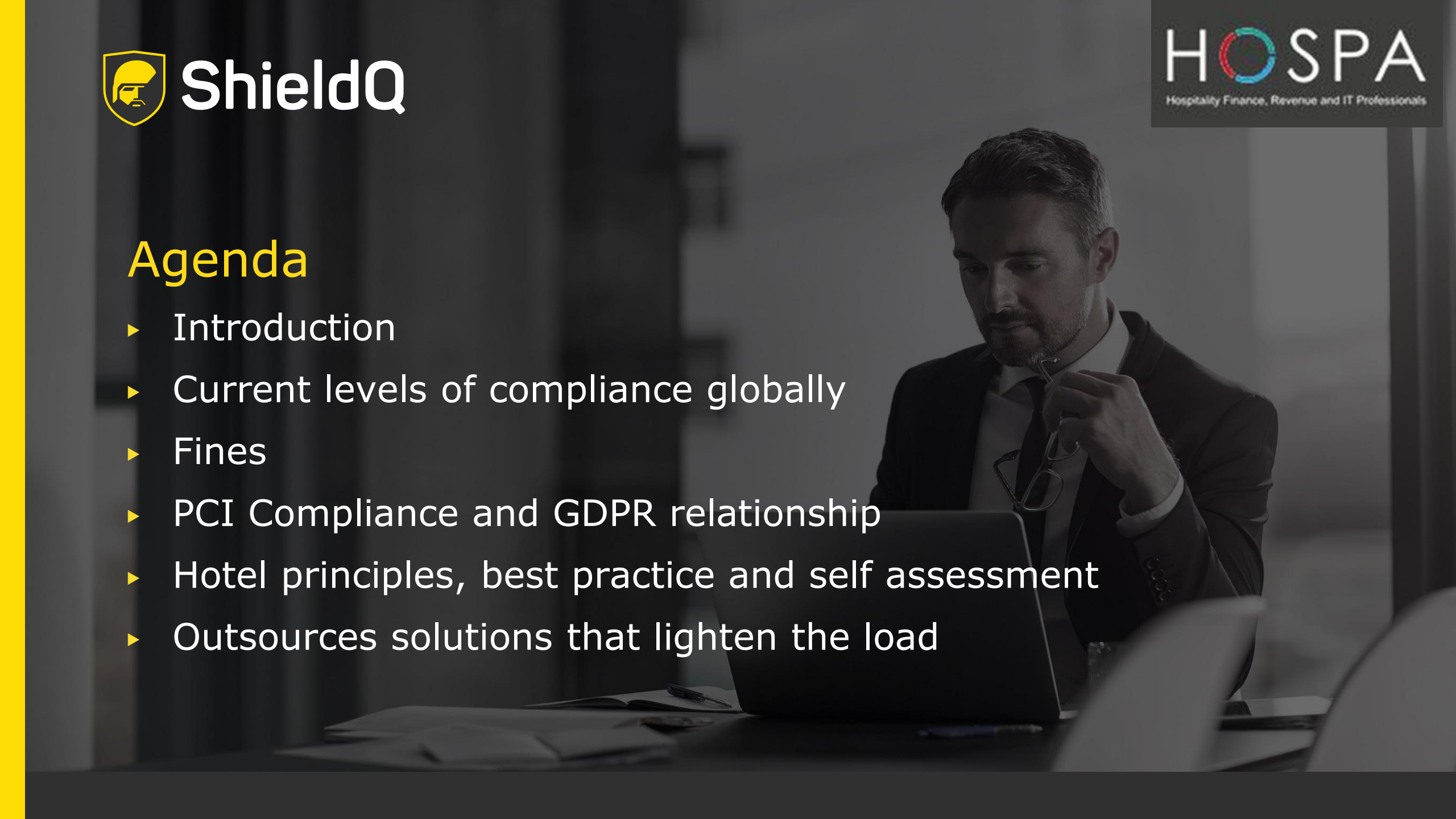
ShieldQ

ShieldQ

HOSPA
Hospitality Finance, Revenue and IT Professionals

Agenda

- Introduction
- Current levels of compliance globally
- Fines
- PCI Compliance and GDPR relationship
- Hotel principles, best practice and self assessment
- Outsources solutions that lighten the load

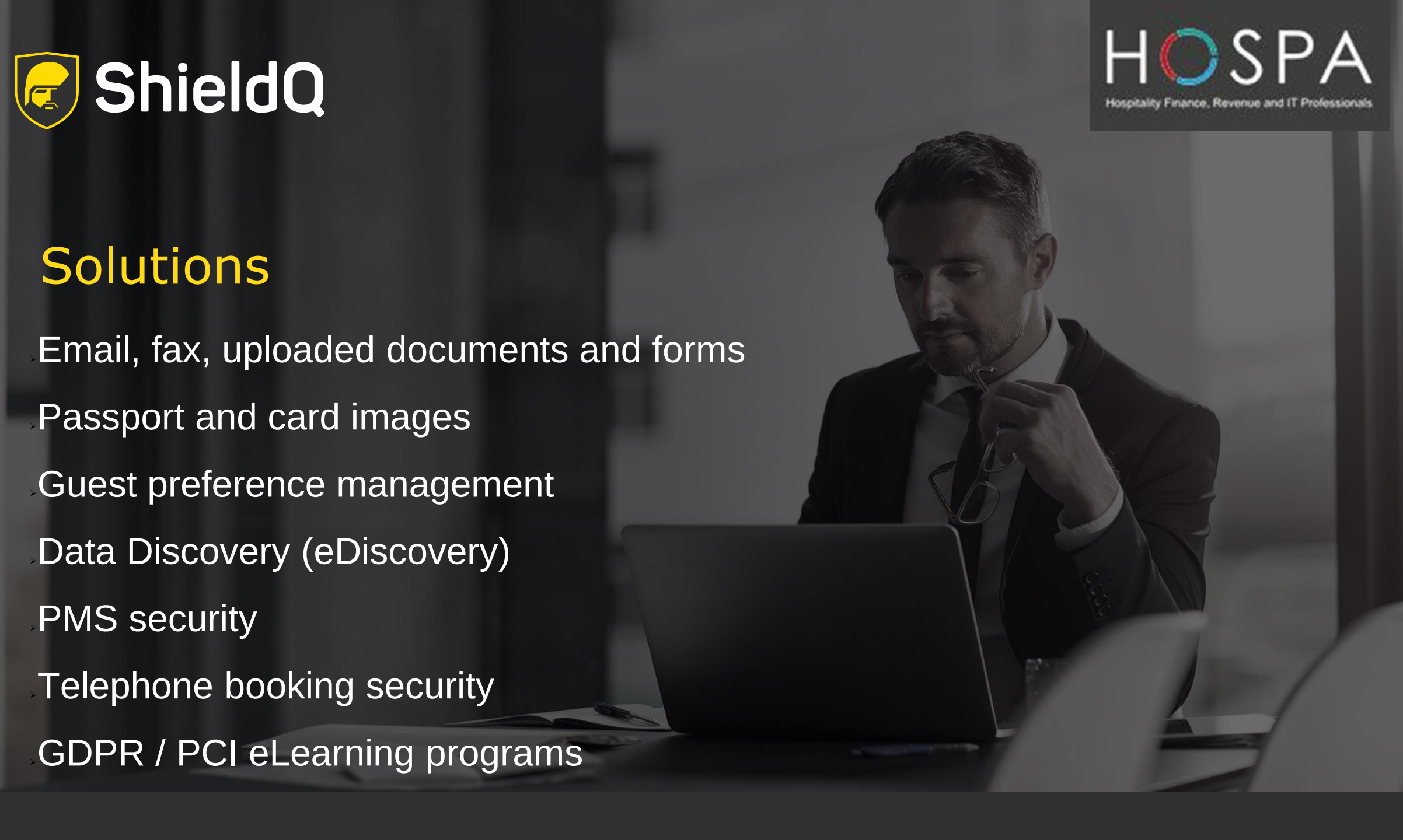


ShieldQ

HOSPA
Hospitality Finance, Revenue and IT Professionals

Solutions

- Email, fax, uploaded documents and forms
- Passport and card images
- Guest preference management
- Data Discovery (eDiscovery)
- PMS security
- Telephone booking security
- GDPR / PCI eLearning programs



ShieldQ

InterFAX
Let the internet do your faxing

PCI BOOKING

ShieldQ

HEDNA

PCI Security Standards Council
PARTICIPATING ORGANIZATION

Member htng

VRMA
Vacation Rental Managers Association

PCI BOOKING

USERS OF PCI BOOKING SOLUTION *(Directly or Indirectly)*

ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals

- General Data Protection Regulations

ShieldQ

HOSPA
Hospitality Finance, Revenue and IT Professionals

Veritas Technologies - 2017

- 900 companies with min. 1,000 employees, 31% meet the minimum standards (global)
- U.S organizations are ahead of those in the U.K. and EU in meeting GDPR compliance.
- Of 200 U.S. companies in the survey, 35% comply,
- Average 20% more expenditure than European companies to comply

PWC Survey - 2017

- 200 U.S. companies with more than 500 employees found 77% plan to spend at least $1 million on GDPR compliance.
- UK 25% behind EU because of Brexit

ShieldQ

HOSPA
Hospitality Finance, Revenue and IT Professionals

PII definition

Personally identifiable information *(PII),* is any information which, either alone or in combination with other pieces of information, can be used to identify or trace a specific individual.

Includes name plus email address, address, social security, NHS, National Insurance, payment card details, Phone ID number (MISN or MIN) and IP address

ShieldQ

HOSPA
Hospitality Finance, Revenue and IT Professionals

Understanding the fines

Hotel with turnover of 2m turnover loses card and CVV numbers for 46,706 Visa and 28,336 MasterCard customers. Under the new Visa policy and GDPR, hotel will pay over £214,000 in fines.

Visa penalty based upon Visa cards impacted and business turnover capped at 5%	£108,776.90
Visa management Fee	£2,197.07
MasterCard penalty (no fine for less than 30,000 cards	£0
Average forensic investigation cost	£12,000
Post-breach compliance report signed by a Qualified Security Assessor (QSA)	£12,000
GDPR Fine @ 4% of turnover	£80,000

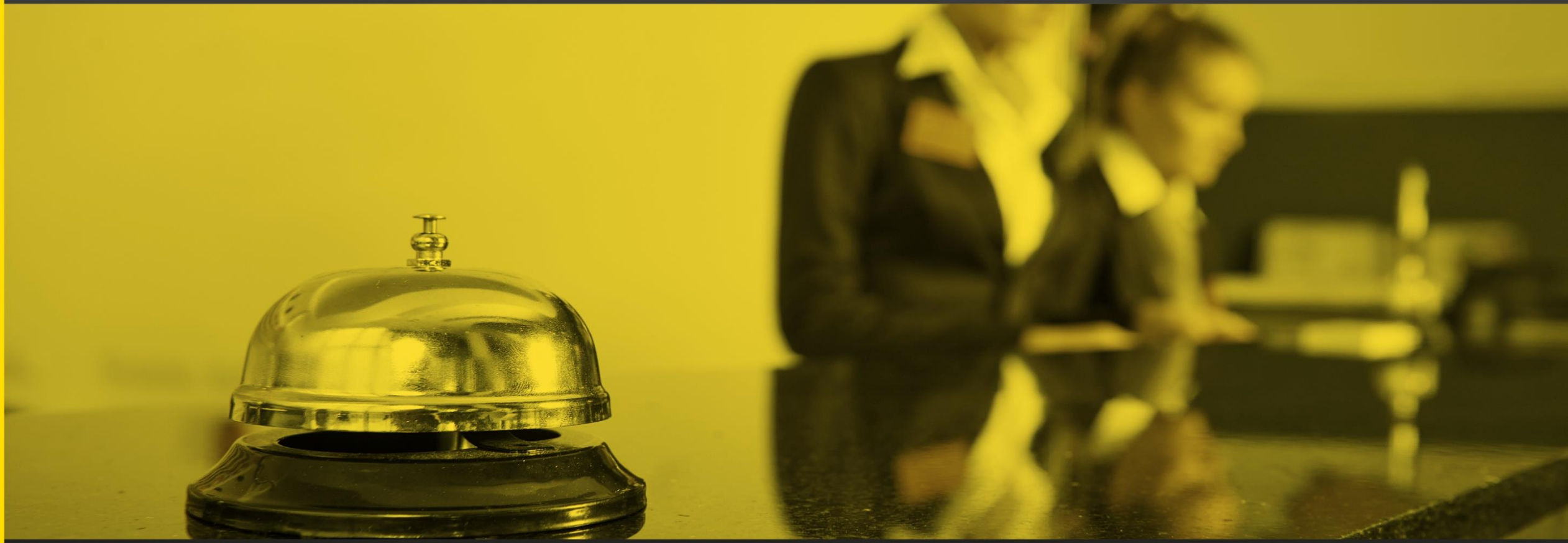
ShieldQ

General data protection regulations *(GDPR)*

- No geographic boundaries
- Fines up to €20m or 4% of global revenue
- Privacy protection in all processes
- Heavy documentation burden
- Risk Assessment
- Grants individuals rights to sue
- 72 hours notification
- National office for monitoring and complaints
- Consent requirements for storage of personal data
- Requires deletion of data if it is no longer used
- National office for monitoring and complaints

ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals



- Hotel Industry Application

ShieldQ

Recommended procedure

- Define the hotels core principles and rationale
- Define the Hotels Guidelines for the collection, Management and PII data
- Define a code of conduct for the hotel and all its staff
- Define audit questions that enable the hotel to self regulate and audit itself against its declared ambitions

ShieldQ

Principles -Do you agree with these statements?

- **Ownership principle**: We recognize that guests own their data and should have a say in how it is used.
- **Regulatory compliance principle**: We obey rules and regulations required by governments and other agencies on guest information.
- **Transparency principle**: In clear and concise terms, we share with the guest the data we hold about them and how it’s being used.
- **Stewardship principle:** We are committed to being good stewards of guest data protecting that data and responding to issues in a timely fashion with a sense of urgency.
- **Partner principle:** We select partners that share our commitment to protect your data

ShieldQ

Personnel questions

- Is guest data used for the purposes in which it was specifically gathered?
- Does the hotel safeguarding guest data make it the responsibility of each and every member of staff their responsibility?
- Are policies and procedures to best protect guest data understood by all relevant staff?
- Are data security issues addressed in accordance with GDPR?
- Does the hotel adequately train employees to follow procedures for protecting guest data ?
- Is a program in place to instruct employees about how to handle sensitive data?

ShieldQ

Website challenges

- Does the website publish a policy and simple to follow procedure when guests are asked to opt-in and out?
- Does the hotel request guest consent to use your data for purposes other than the primary business needs ?
- Does hotel use clear language?
- Does the hotel make the information about the data the hotel collects easily accessible?
- Can guests remove any data that is no longer required to be kept?

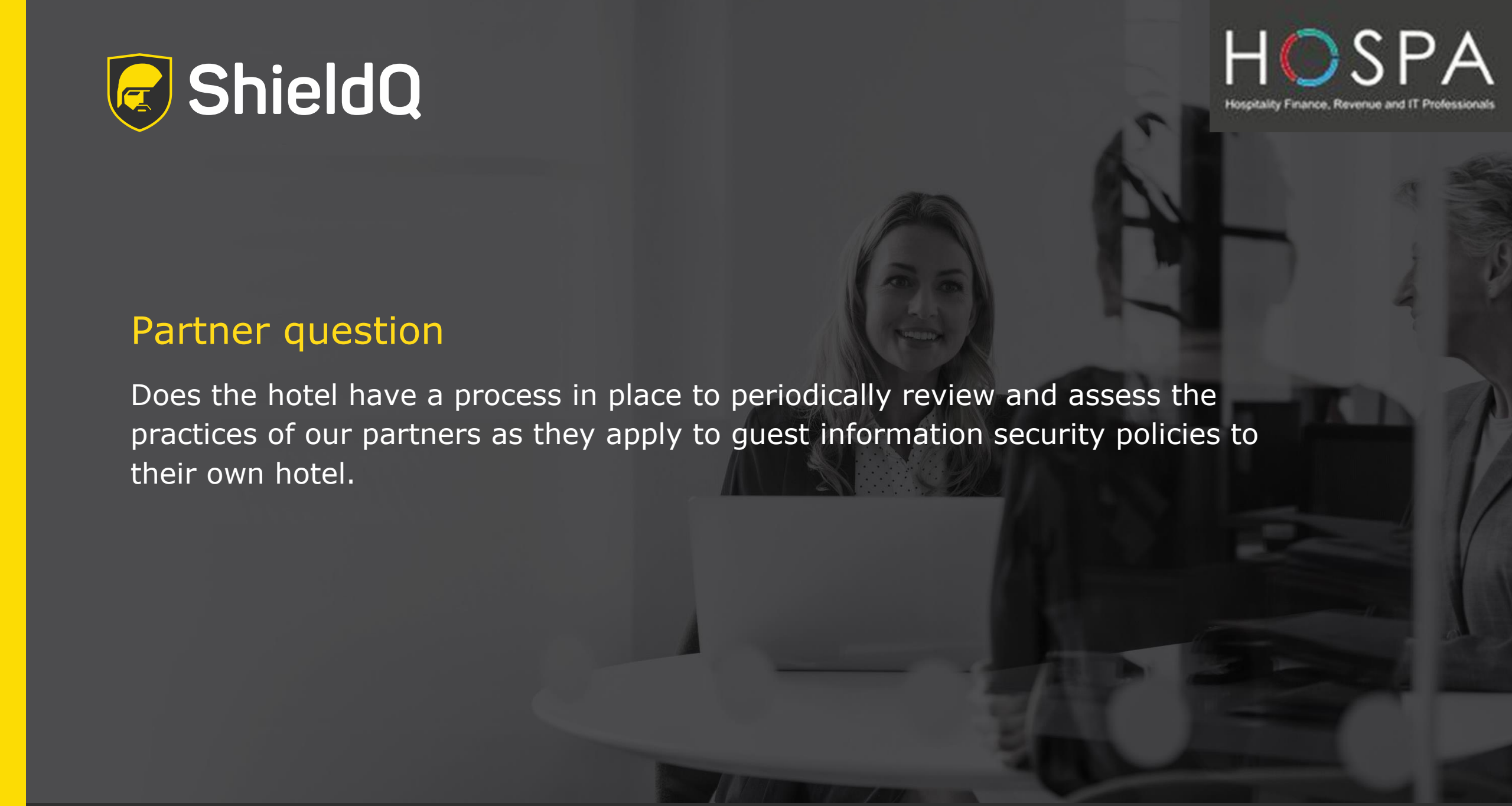
ShieldQ

Website challenges *(continued)*

- Does the hotel request guest consent to use guest data for purposes other than the primary business need?
- Are different policies applied to each jurisdiction in which the hotel operates?
- Does the hotel make it easy for guests to request corrections to information a hotel stores?
- Does the hotel inform guests of the status of the requested change?
- Does the hotel communicate how long the hotel keeps guest data?

ShieldQ

HOSPA
Hospitality Finance, Revenue and IT Professionals



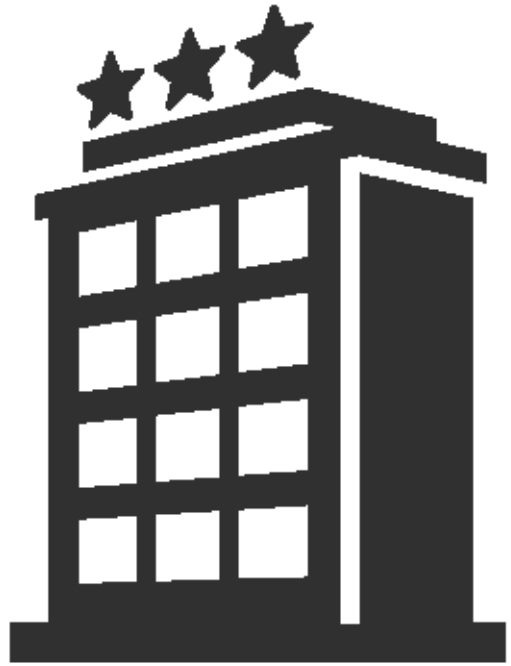
Partner question

Does the hotel have a process in place to periodically review and assess the practices of our partners as they apply to guest information security policies to their own hotel.

ShieldQ

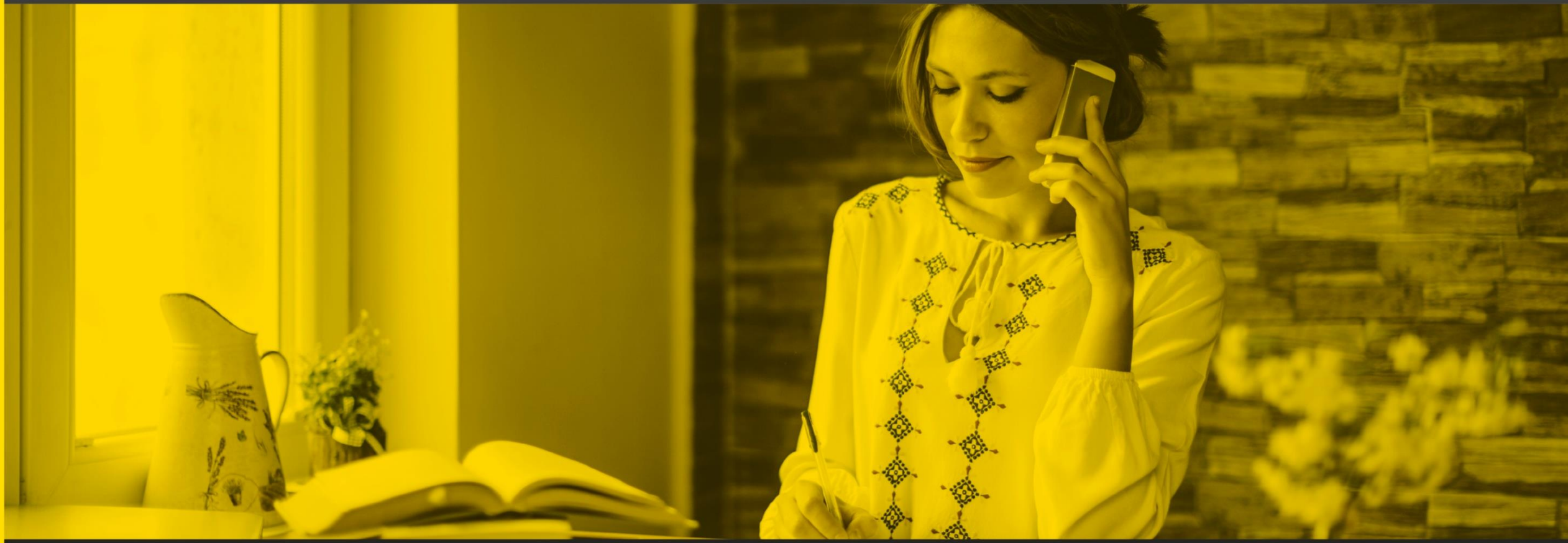
Hotel data questions

- Where is the sensitive data stored?
- What can we delete, redact, quarantine, encrypt?
- What data do we need to keep accessible to staff?
- What is retention policy and how is it applied?
- Where does it move from and too?
- Who needs access to it and how?
- How do we constantly remove data we don’t want



ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals



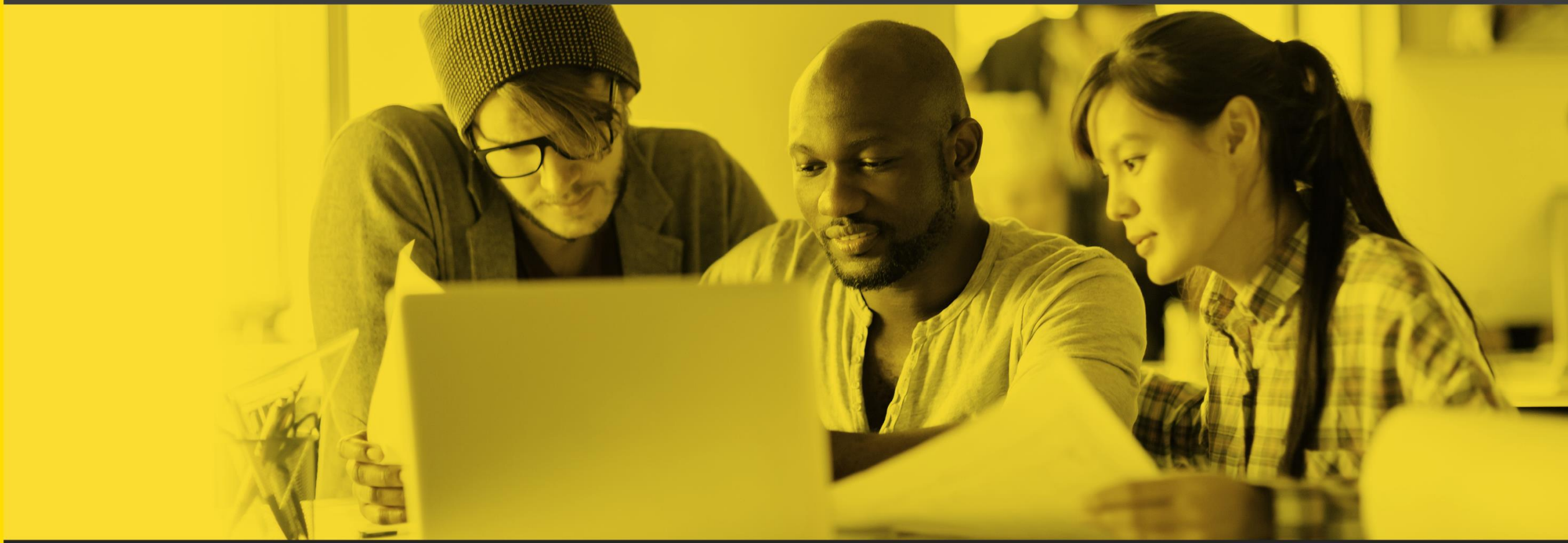
- PCI compliance questions

PCI questions

- **Do I have an AOC** *(not SAQ)* **from my core suppliers?**
  - PMS system
  - CRS system
  - Channel Manager
  - Booking Engine
  - POS
- **Are my front desk operations compliant**
  - Telephone bookings
  - Fax management
  - Email management
  - Concierge operations
  - Banqueting / events
  - Spar / golf / other

ShieldQ
Delivering data compliance

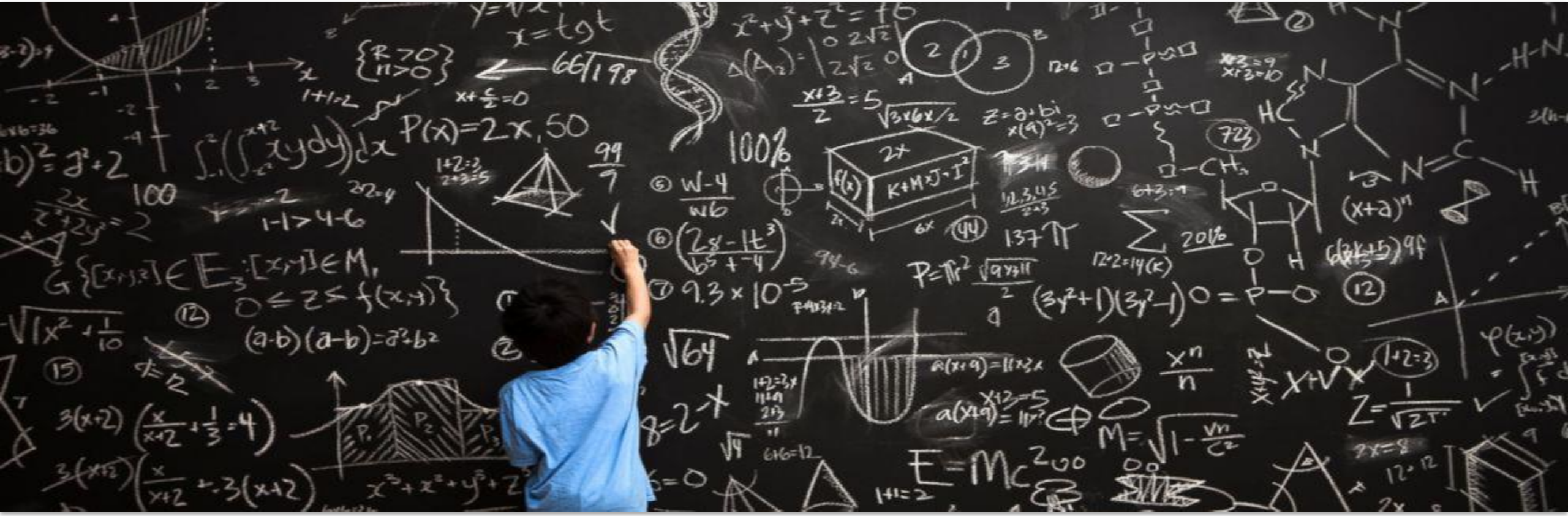
HOSPA
Hospitality Finance, Revenue and IT Professionals



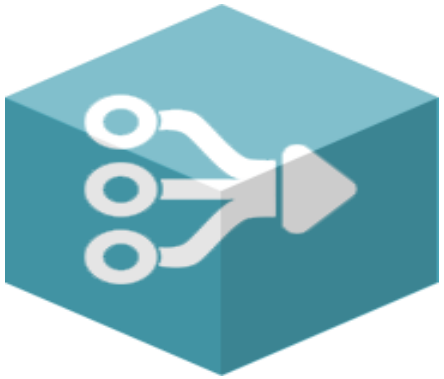
- Guest preferences and consent

PrivacyCheq

Create and package ready-to-implement notice/consent solutions to operationalize GDPR compliance



PrivacyCheq



Logging Compliance

Managing Rights

Prove Compliance

Parental Consent

Notice

Reporting

Logging Compliance

- Verify GDPR Applicability (Article 1)
- Verify GDPR Relevance (Articles 2 & 3)
- Verify Legal Basis for Data Processing (Article 6)
- Implement “Data Minimization” (Article 5)
- Implement “Storage Limitation” with respect to duration (Article 5)
- Respect Data “Accuracy” (Article 5)
- Respect Data “Integrity” (Article 5)
- Maintain Data “Confidentiality” (Article 5) Implement Data Breach Procedures (Articles 33 & 34)
- Eliminate Need for Parental Consent (Article 8)
- Determine Applicability of Legitimate Interest (Article 6)
- Gather Informed Consent (Articles 5, 6, 7, 13 & 14)
- Gather Informed Consent for “Processing which does not require identification” (Article 11)
- Evaluate use of anonymous consent (Article 11)
- Gather consent to process “special category” data (Article 9)
- Gather Parental Consent (Article 8)
- Gather Consent for Automated Processing (Article 22)
- Manage Direct Marketing Objections (Article 21)
- Present Appropriate Notice (Article 7)
- Implement Withdrawing Consent (Articles 7 & 17)
- Comply with GDPR requirement “It shall be as easy to withdraw Consent as to give it” (Article 7)

Managing Rights

- Implement Privacy by Design Principles of “Lawfulness, Fairness, and Transparency” (Article 5)
- Implement “Data Minimization” (Article 5)
- Implement “Storage Limitation” with respect to duration (Article 5)
- Respect Data “Accuracy” (Article 5)
- Respect Data “Integrity” (Article 5)
- Maintain Data “Confidentiality” (Article 5)
- Implement Data Breach Procedures (Articles 33 & 34)
- Implement Parental Consent (Article 8)
- Manage Direct Marketing Objections (Article 21)
- Manage Consent Withdrawal (Article 7)
- Maintain Records of Consent (Article 7)
- Provide Copies of Personal Data (Article 15)
- Communicate Rectification of Personal Data (Article 16)
- Implement Data Portability Procedures (Article 20)

Parental Consent

- Verify that the data subject is a child (Articles 8 & 40)
- Verify that data subject giving consent is an adult (Articles 8 & 40)
- Verify that data subject giving consent holds “parental responsibility” over child (Articles 8 & 40)
- Inform parent about personal data collected from child (Articles 8 & 40)
- Gather consent from parent (Articles 8 & 40)
- Provide parent ability to view and maintain child’s personal data (Articles 8 & 40)
- Provide parent ability to revoke their consent to process child’s personal data (Articles 8 & 40)

Prove Compliance

- Verify GDPR Applicability (Article 1)
- Verify GDPR Relevance (Articles 2 & 3)
- Maintain Legal Transfers of personal data from the EU (Articles 44, 45, 46 & 47)
- Create Privacy Impact Assessments (Article 35)
- Record Consent (Article 7)
- Demonstrate Cooperation with Supervisory Authorities (Articles 55 & 56)
- Demonstrate Compliance with a Code of Conduct (Article 40)
- Maintain Records of Consent (Article 7)
- Maintain Records of Consent Date and Time (Article 7)
- Maintain Records of Consent Events (Article 7)
- Maintain Record of the Notice Consent was given for (Article 7)

Reporting

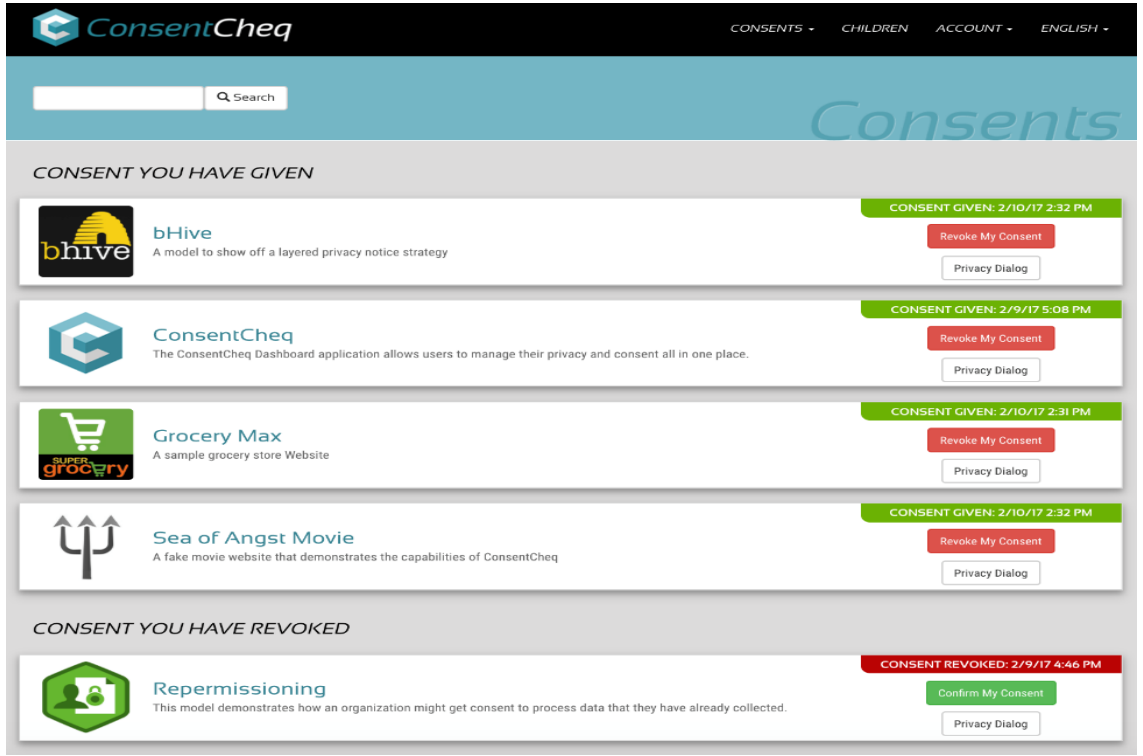
- Create Database for Notice Consent Event Storage (Article 55)
- Report Records of Consent (Article 7)
- Report Records of Consent Date and Time (Article 7)
- Report Records of Consent Events (Article 7)
- Report Records of the Notice Consent was given for (Article 7)
- Demonstrate Cooperation with Supervisory Authorities (Article 55)

Notice

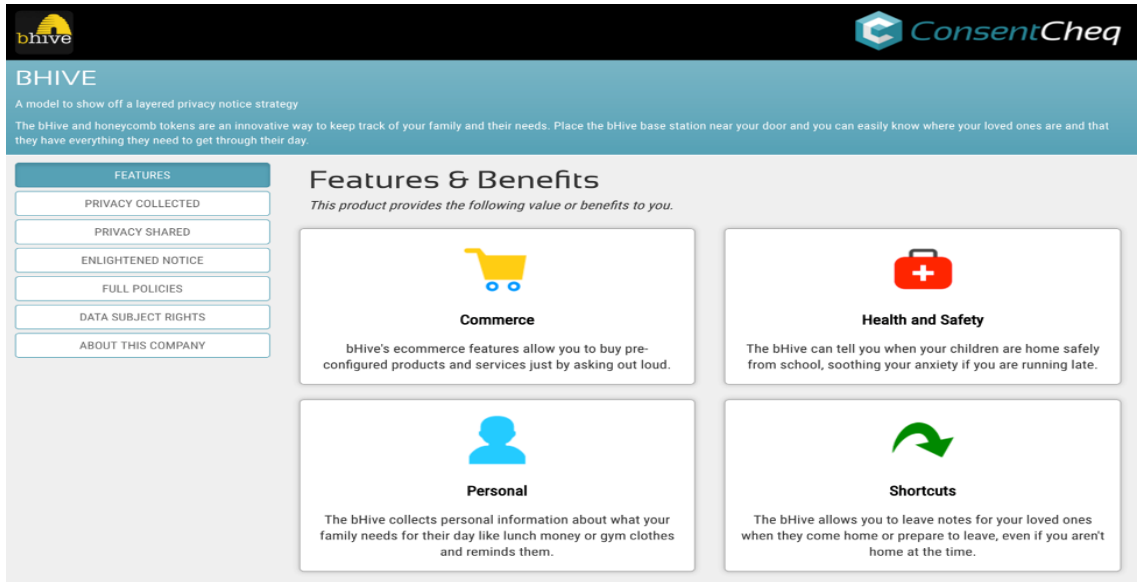
- Comply with GDPR requirement for “explicit” notice (Article 12)
- Comply with GDPR requirement for “specific” notice (Article 12)
- Comply with GDPR requirement for “informed” notice (Article 12)
- Comply with GDPR requirement for “concise” notice (Article 12)
- Comply with GDPR requirement for “transparent” notice (Article 12)
- Comply with GDPR requirement for “intelligible” notice (Article 12)
- Comply with GDPR requirement for “easily accessible” notice (Article 12)
- Comply with GDPR requirement for “using clear and plain language” notice (Article 12)
- Prepare for implementation of standardized icons (Article 12)
- Reveal legal basis under which personal data was collected (Articles 13 & 14)
- Describe purpose for collecting personal data (Articles 5, 13 & 14)
- Inform data subject who is collecting the data (Articles 13 & 14)
- Include data privacy officer’s contact information (Articles 13 & 14)
- Reveal name and location of any data processors (Articles 13 & 14)
- Reveal how long the data controller will keep the personal data (Articles 13 & 14)
- Ensure request for consent is clearly distinguishable from other matters (Article 7)
- Document source of data that is not collected directly from the data subject (Article 14)
- Disclose the existence of the right to be forgotten (Articles 13 & 14)
- Disclose the right to lodge a complaint with supervisory authorities (Articles 13 & 14)
- Provide notice of need to collect personal data (Articles 13 & 14)
- Disclose where data controller intends to further process the data (Articles 13 & 14)
- Inform consent for automated processing (Article 22)

ConsentCheq

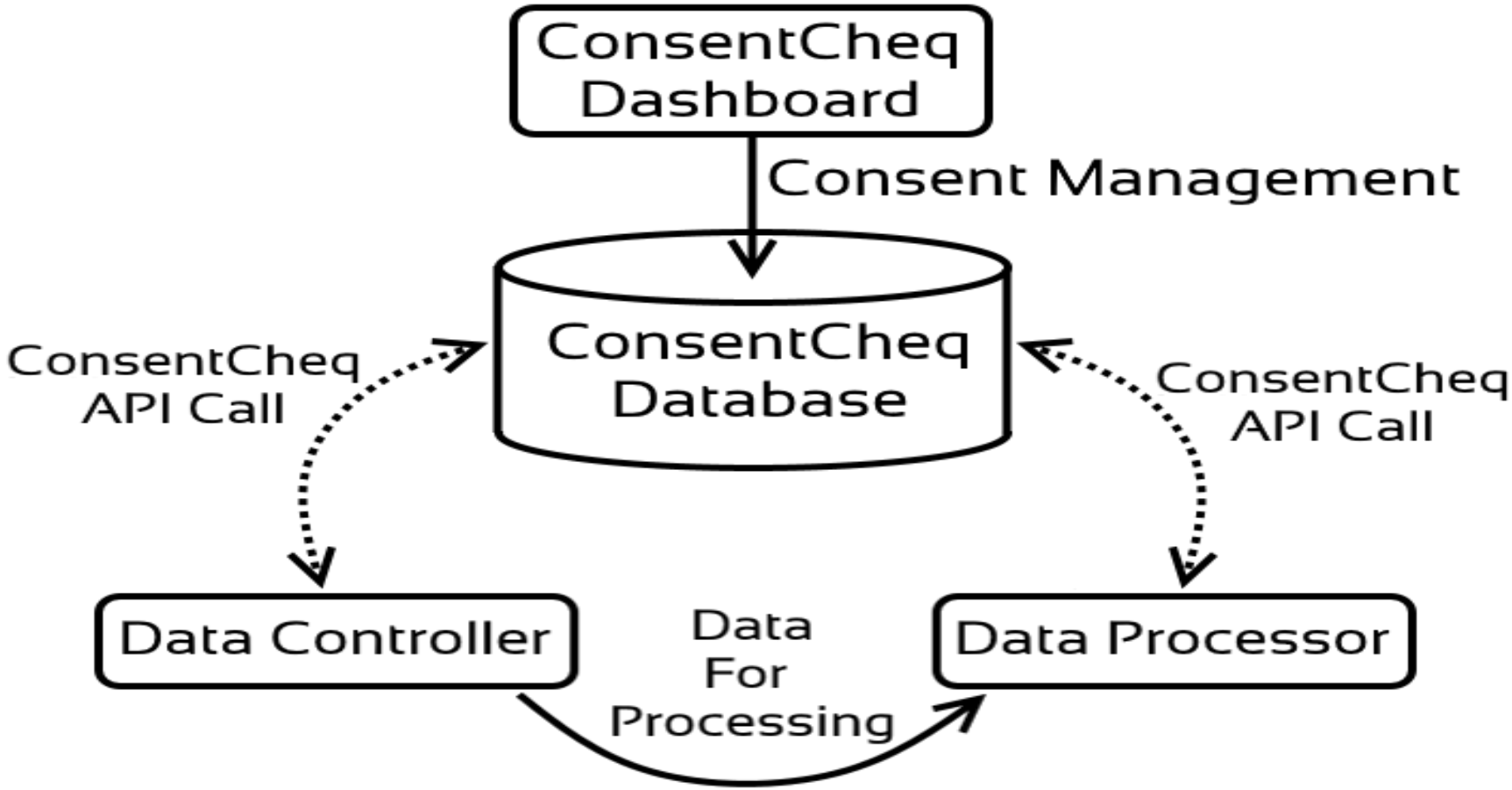
Compliance Development Kit



- Gives data subjects a portal to manage their rights under the rule
- Provides verifiable parental consent



- Generated by a survey
- Does not require technical skills
- Provides an answer to the “aspirational” requirements for notice in Article 12


ConsentCheq
Dashboard
Consent Management
ConsentCheq
Database
ConsentCheq
API Call
ConsentCheq
API Call
Data Controller
Data
For
Processing
Data Processor

- PrivacyCheq is developing **CRM connectors** for companies to edit customer personal data stored in CRM solutions

- Currently companies can set up a **URL request** and/or **e-mail request** for notifications when a change to consent status occurs

ConsentCheq Operationalizes GDPR Compliance with:

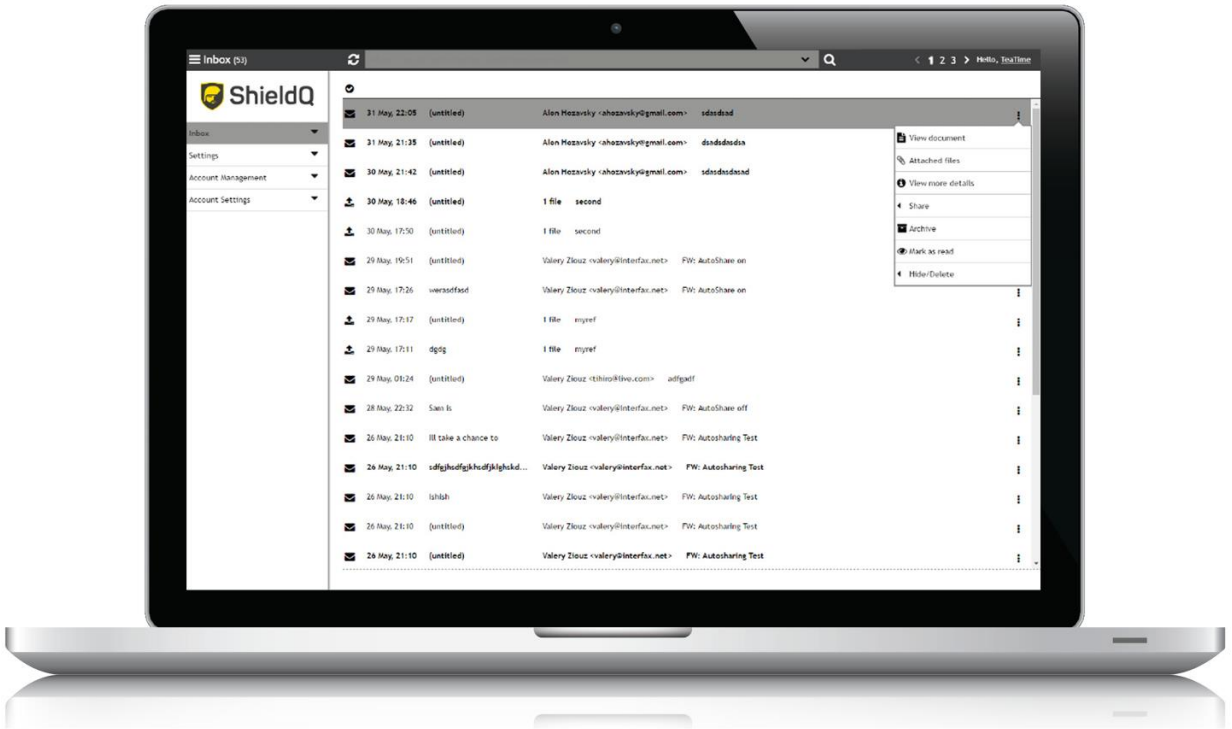
- **Privacy Dialog**: The ability to generate concise, plain-language, graphical privacy policy briefs to augment full privacy policies with no coding effort
- **Compliance Logging Solution**: Cloud-based consent management database and API to allow apps and websites to obtain consent and understand scope and status of a data subject's wishes regarding their rights in real-time
- **Data Subject Consent Choice Management Dashboard**: A website for data subjects to manage their ongoing consent choices under the GDPR
- **Proof of Concept:** Hypothetical use cases simulating consumer-facing personal data contact across different use cases

ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals

- Secure document management

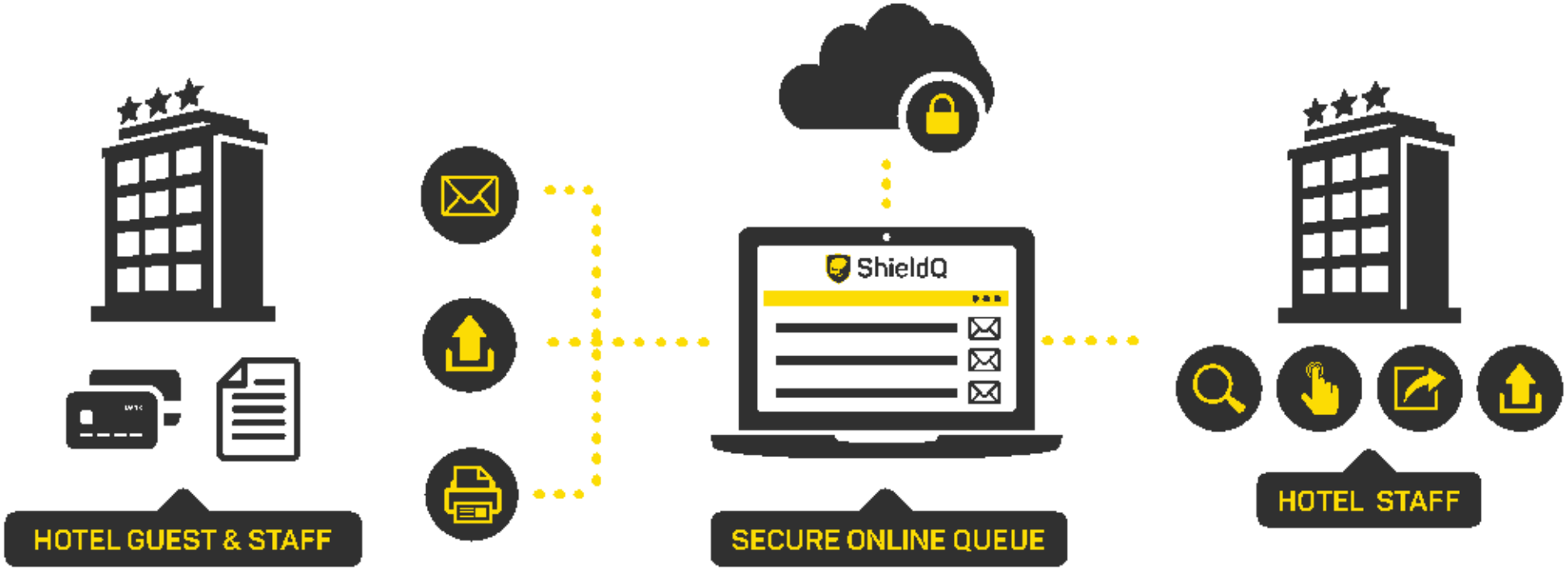
ShieldQ


Inbox (53)
ShieldQ
Inbox
Settings
Account Management
Account Settings
View document
Attached files
View more details
Share
Archive
Mark as read
Hide/Delete


GRSEE
This is to Certify that
InterFAX
is a PCI DSS level 1 service provider
and that its online service solutions
were found to meet all of PCI DSS
requirements and is qualified as
PCI DSS Compliant
This certification relates to
Version 3.1 of the PCI standard
Valid 11 Nov, 2015 through 10 Nov, 2016

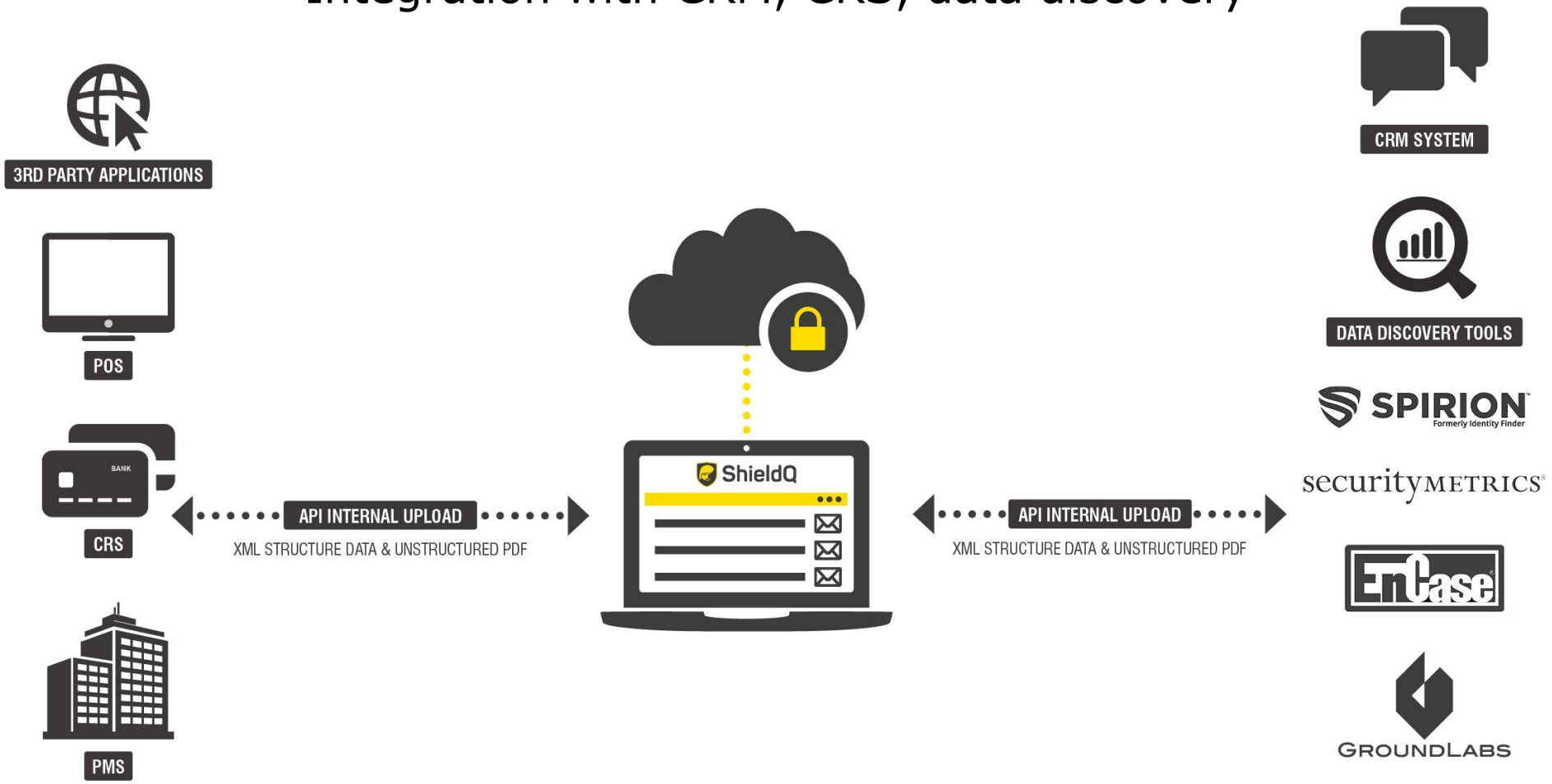
ShieldQ

Emails, fax, uploaded form bookings, passports, photos, credit card images, authorization forms and ID



ShieldQ

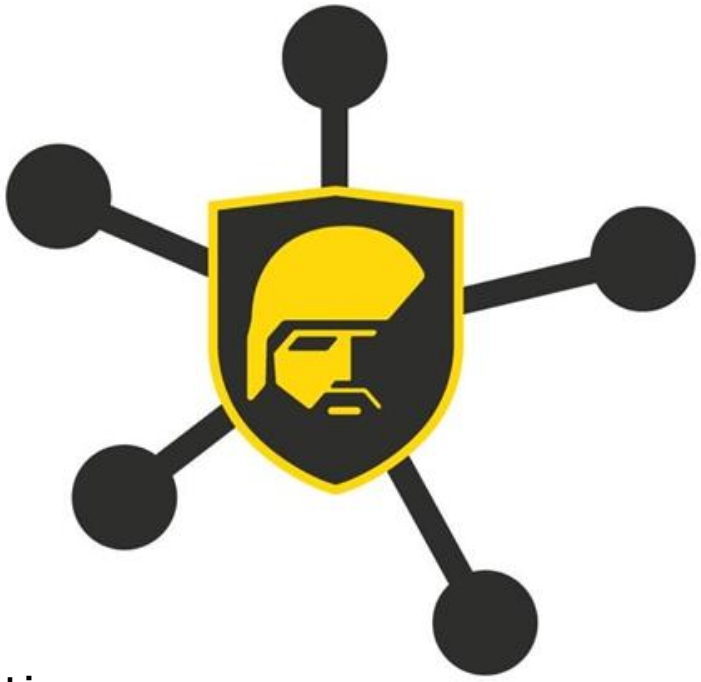
Integration with CRM, CRS, data discovery



ShieldQ

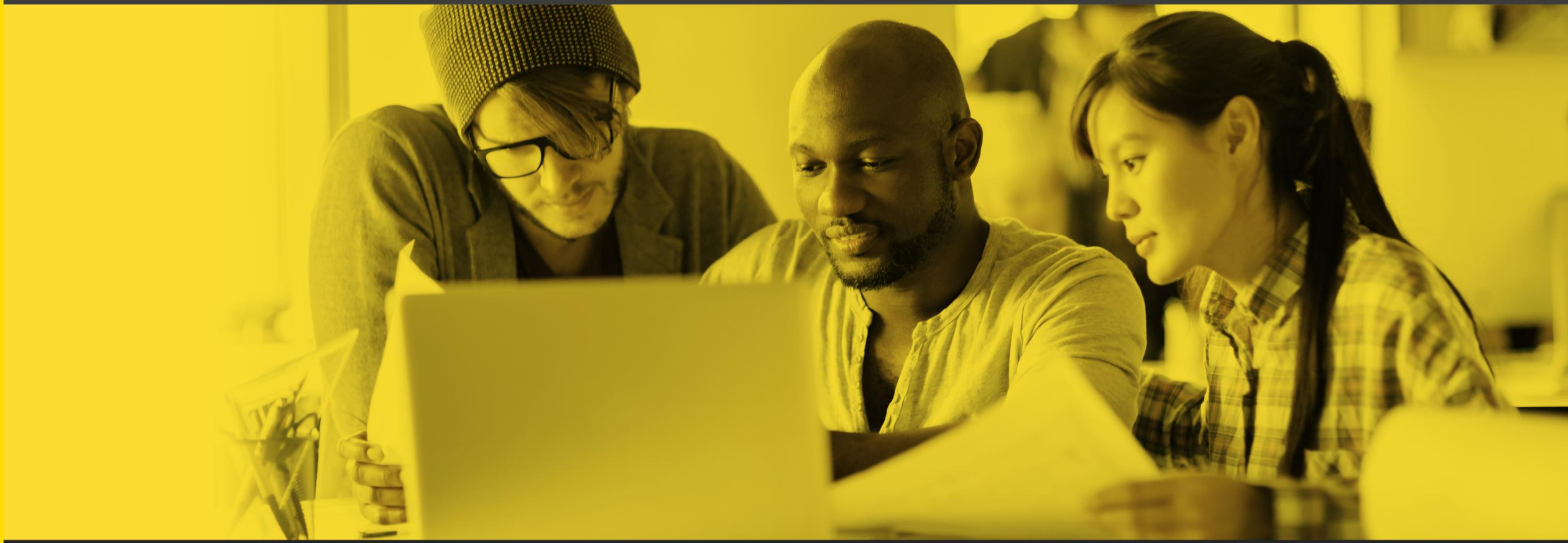
Benefits

- Legacy security weaknesses identified and fixed
- All unwanted data at risk destroyed
- All essential PII and card data retained in secure storage
- Search and recovery using simple XML and API interface
- Flexible document sharing, and archiving features
- Powerful custom document delete features
- Minimal disruption to business continuity
- Maximum security
- No change to existing workflows
- Very low cost
- Enhanced AWS service – encryption, search and sharing functions



ShieldQ
Delivering data compliance

EXHIBITING AT:
HITEC 2016
Produced by HFTP

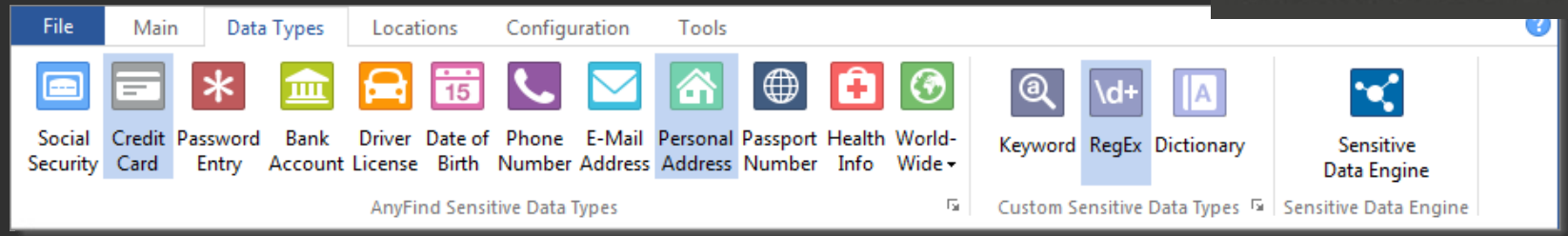


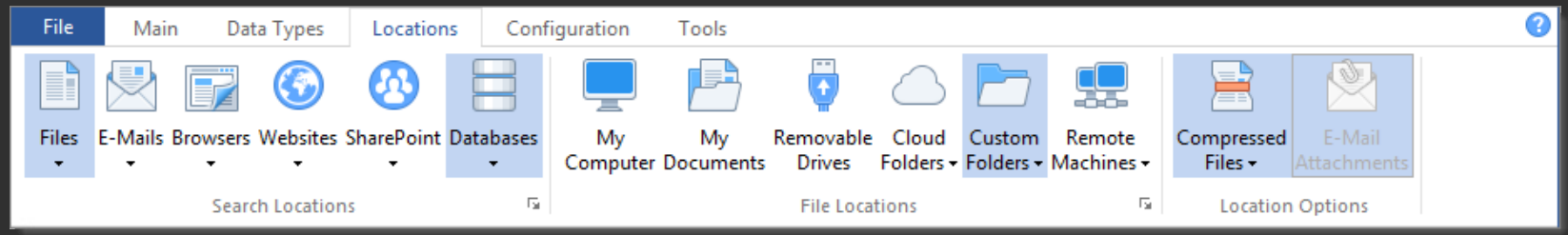
- Data discovery

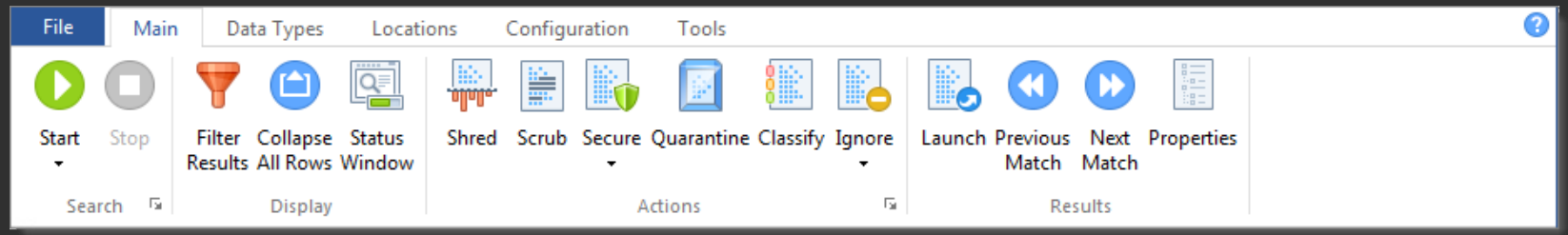
ShieldQ
Delivering data compliance

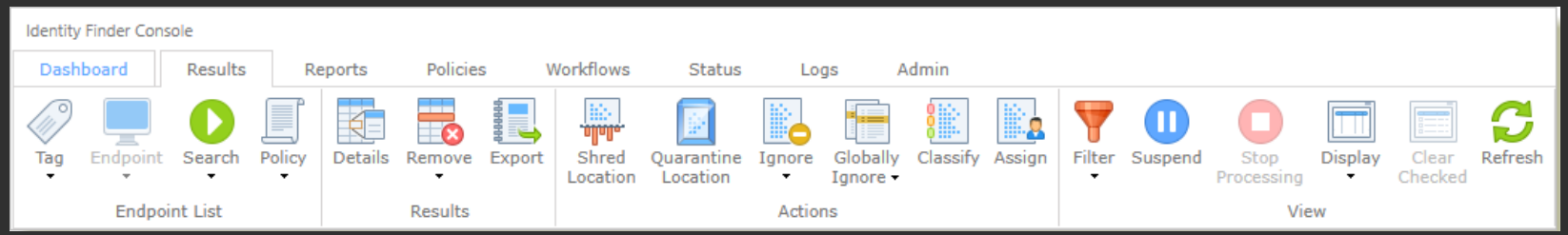
HOSPA
Hospitality Finance, Revenue and IT Professionals

Data discovery









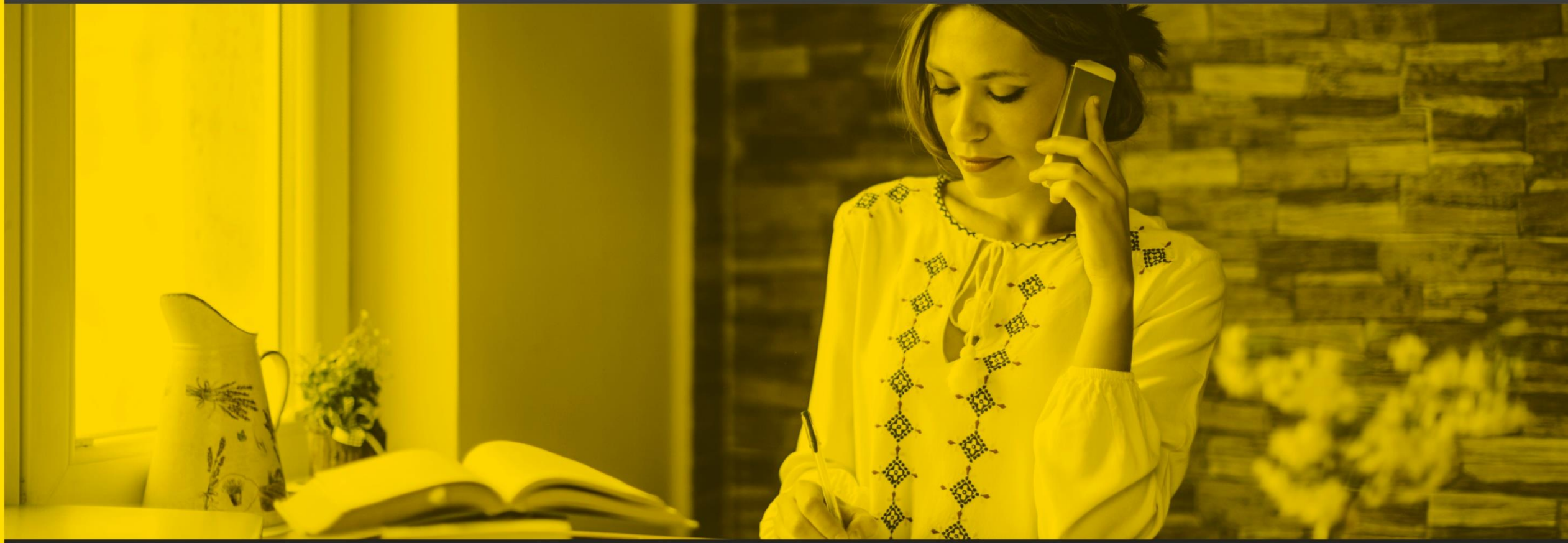
ShieldQ

Data discovery search

- All data types – typically 100 different data strings searched
- Search any file format *(encrypted and unencrypted)*
- Periodic or perpetual usage
- Plug the leaks and prevent ongoing repeat accumulation of unwanted data
- Delete, redact, encrypt or quarantine sensitive data
- Convert sensitive records
  - Unstructured data convert to PDF
  - Structured sensitive data to XML
- Upload *(and download)* above to 'ShieldQ'
- Search and retrieve data from PCI / GDPR environment using legacy systems

ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals



- PCI compliance questions

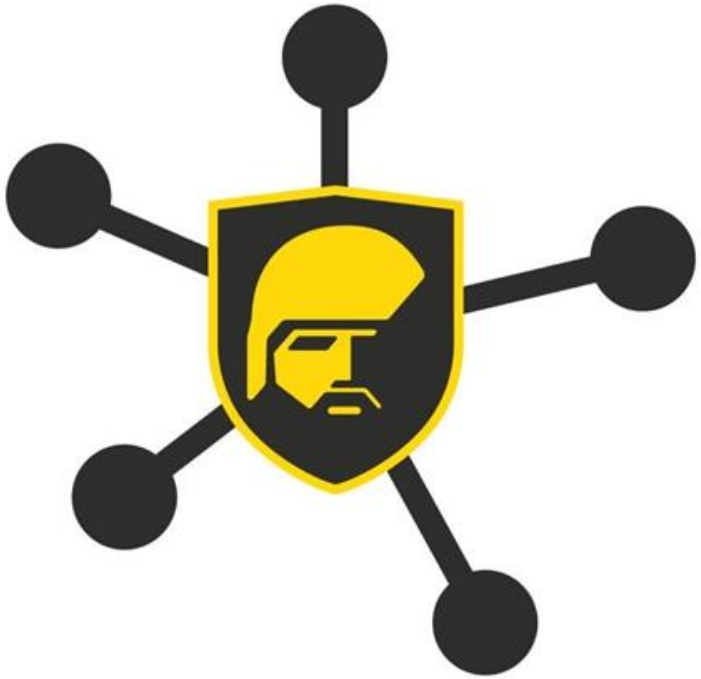
ShieldQ

PMS PCI Compliance

- Free API removes all PMS vendors from scope
- Nominal payment for by hotel by DD / Card

Features:

- Tokenization on the fly
- Payment capture iframe
- iFrame payment display
- Payment through universal payment gateway
- Multiple payment gateways
- PDQ integration
- Telephone payments



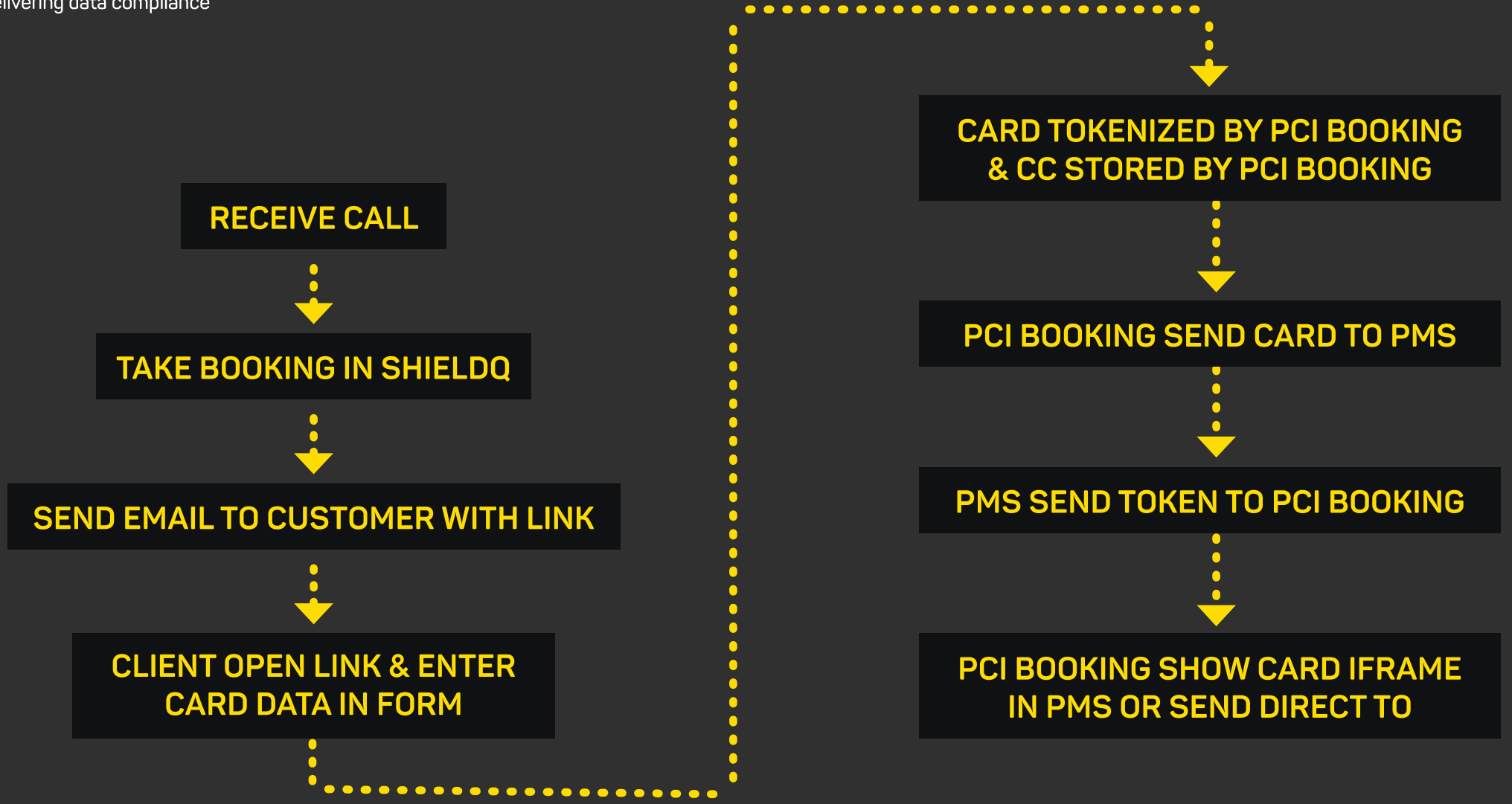
ShieldQ
Delivering data compliance

HOSPA
Hospitality Finance, Revenue and IT Professionals

Telephony

ShieldQ

Delivering data compliance



ShieldQ

Accreditation

ShieldQ

Delivering data compliance

Here to help!

Get in touch today, to discuss your PCI compliance needs:

+353 1 905 8968

geoff@shieldq.com

shieldq.com