KPMG

The UAE Privacy Regulatory Landscape

How can UAE businesses comply with the UAE Federal Data Protection Law (Law No 45 of 2021).

KPMG Lower Gulf

12 Jan 2022

Agenda

1 **Introductions**

2 **Overview of the Evolving Landscape in the UAE**

3 **UAE Federal Data Protection Law**

4 **Implementing an Effective Data Privacy Program**

5 **OneTrust Platform – Automating Privacy**

01

Introductions

Introductions

Maliha Rashid
Director | Data Privacy Lead
KPMG Lower Gulf

Maliha leads our data privacy services for KPMG Lower Gulf. Maliha has over 18 years of experience in Cybersecurity and Data privacy across France and the Middle East. She supports clients across all industries in the UAE in their privacy journeys.

Alexis Kateifides
Senior Centers of Excellence Counsel

Alexis assists with the development of tools and resources that provide privacy professionals with the ability to make informed choices regarding the intricacies of international data protection compliance.

Kristof Ruisz
Privacy Adviser

Kristof is a data protection and privacy advisor for the Emirates Group. He has a law degree and is skilled in privacy and data protection legal and compliance and privacy program management.

02

Overview of the evolving landscape in the UAE

The UAE data protection regulatory landscape is evolving rapidly

1. UAE Federal Data Protection Law

The UAE has enacted a **new Federal Data Protection Law to** drafted in partnership with major technology companies. The Law constitutes a significant development in modernizing the UAE's onshore data protection laws and will empower individuals to control how their personal data is processed.

2. DIFC-Data Protection Law

DIFC Data Protection Law of 2020 law prescribes rules and regulations regarding the collection, handling, disclosure and use of personal data in the DIFC, and the rights of individuals to whom the personal data relates.

3. Abu Dhabi Global Market (ADGM)

ADGM's Data Protection Regulations 2021 require every ADGM registered entity that processes personal information to register with the Office of Data Protection at the Registration Authority and renew its registration annually.

4. UAE Central Bank Consumer Rights

The Central Bank of the UAE (**CBUAE**) has issued Consumer Protection Regulation and associated Standard, which is the foundation of its new Financial Consumer Protection Regulatory Framework (FCPRF) and aims to ensure protection of consumers.

5. Federal Law By Decree 3 Of 2003

Regulating Telecommunications (**Federal Law by Decree 3 of 2003** as amended), which includes several implementing regulations/ policies enacted by the Telecoms Regulatory Authority ('TRA').

6. Federal Law No. 2 Of 2016 On Combating Cybercrimes

The **Cyber Crime Law** protects the privacy of information published online including data, information, credit card numbers, bank account statements and details of electronic payment methods.

7. Internet Access Management Regulatory Policy-TRA

The TRA monitors online content available to users in the UAE and will draw to the attention of website operators based in the UAE any potential breaches of the **IAM** policy.

8. Abu Dhabi Digital Authority

ADDA promotes the principles of accountability and transparency across Abu Dhabi government and public entities. **The Data Management Policy by ADDA** covers Data Security and Privacy domains for Abu Dhabi Government entities.

9. UAE-Federal Law No. 2 of 2019 to Protect Health Data

UAE has issued **Federal Law No. 2 of 2019**, Concerning the use of the Information and Communication Technology in the Area of Health ("**ICT Health Law**").

03

KPMG & OneTrust counsel deliver thoughts on new UAE Data Protection Law

What does the UAE Federal Data Protection Law cover ?

The **Federal Data Protection Law 2021** came into force on the **2nd Jan 2022**.

The purpose of this law is to provide standards and controls for the processing and free movement of Personal Data by Controller or Processor and to protect the fundamental rights of Data Subjects, including how such rights apply to the protection of Personal Data in emerging technologies.

01

General provisions: Definitions, Objectives & Scope of Application of the Decree-Law

02

General rules for data processing: Controls of Processing personal & Sensitive Data

03

Conditions of consent & obligations of the controller and processor: Terms & Obligations

04

Data protection officer: Appointment & Duties of the Data Protection Officer

05

Data owner rights: Right to Withdraw, Right to Access & Rectify, Right to Object Processing, etc. (Refer to slide 14)

06

Data security and assessment of the impact of its protection: Personal Data protection risks and Impacts

07

Cross-border transfer of personal data: Data Sharing & Complaints Processes

08

Final provisions: Fines, Executive Decisions, Publication & Implementation of the UAE Federal Law and the Data Office.

Where is the UAE DP Law Applicable and who does it apply to?

1

The DP Law applies to:

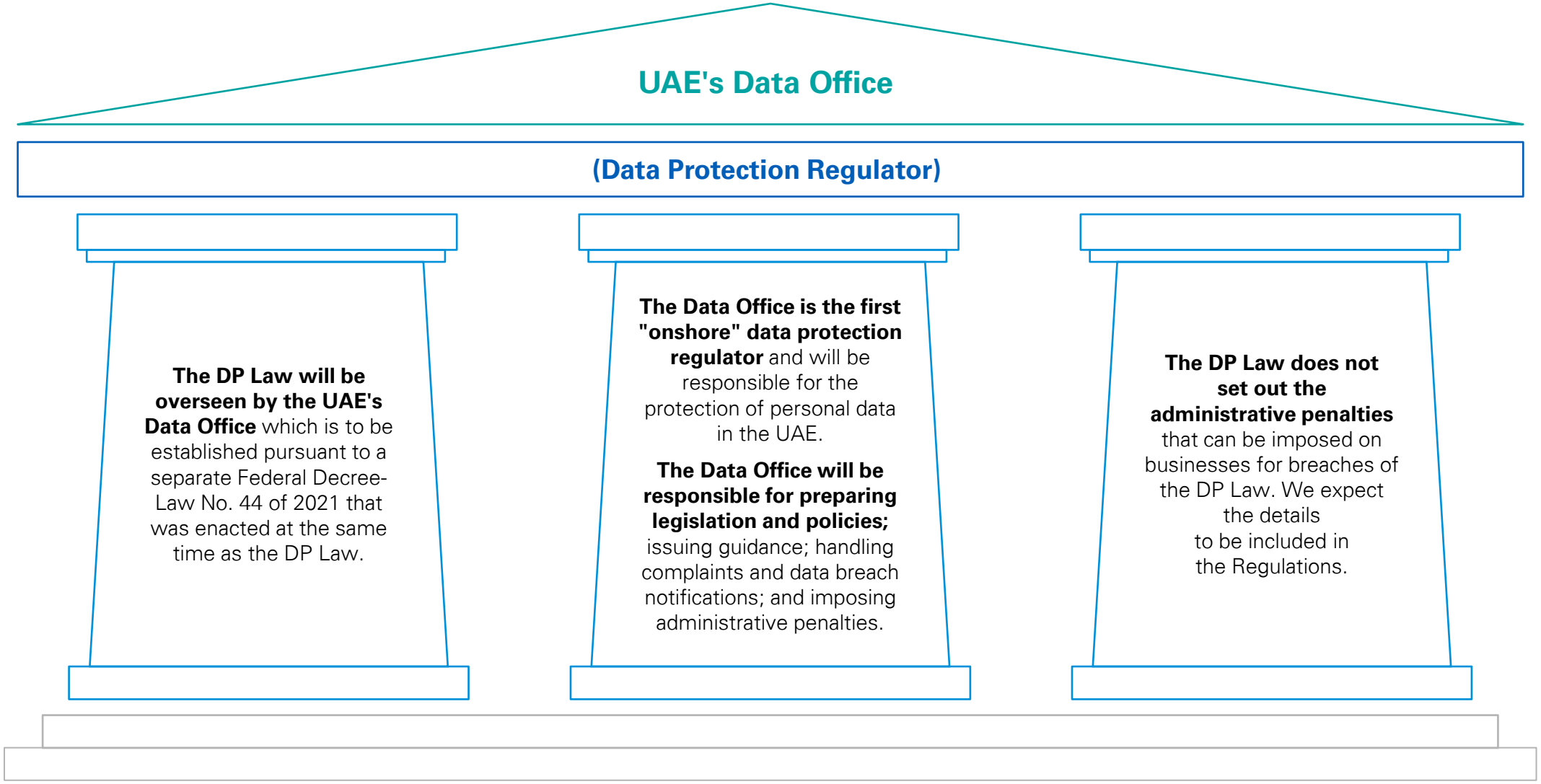
- All businesses that are processing personal data in the UAE (irrespective of whether the personal data relates to data subjects inside the UAE).
- Businesses that are based abroad but are processing personal data relating to data subjects that are inside the UAE.
- The new DP Law therefore has an "extra-territorial" reach similar to the GDPR.

2

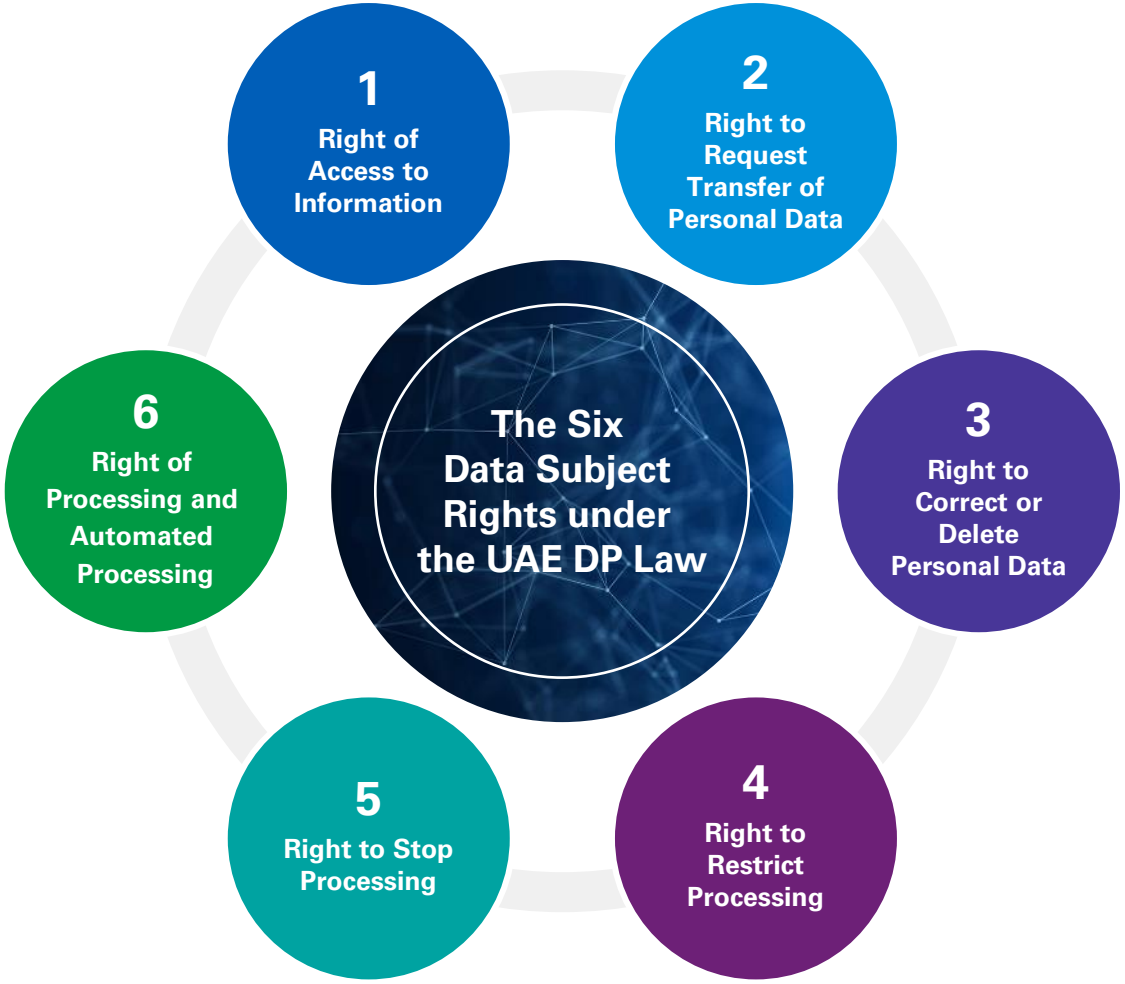
The DP Law does not apply to:

- Banking personal data as there are separate regulations (CPR & CPS of CBUAE) for the protection of such data.
- Entities in UAE free zones where such free zones have their own data protection and privacy laws (such as DIFC & ADGM).
- Government data & Government authorities that control or process personal data.
- Personal health data where there is separate legislation covering such personal data.

Who will be responsible for regulating the new UAE DP Law?



What individual rights does the UAE Federal DP Law set out?



UAE Federal Data Protection Law vs GDPR?

Key: Similar: = Absent: X Broader: () Narrow:)(

Domain	GDPR	Key	UAE Federal Data Protection Law
Material and Territorial Scope	Personal data collected in the EU/EEA i.e. "EU personal data". The GDPR also has **extra-territorial reach**.	=	Data subjects who reside in the UAE or has a place of business there. The new DP Law has an **extra-territorial** reach similar to the GDPR.
Governance/ DPO	**Appoint a DPO** and lead supervisory authority u**nder certain conditions.**	=	Companies will need to **appoint a DPO under certain circumstances**. The DPO may be an employee of the company or an external party.
Penalties	Up to **20m** or **4% of global annual revenues**.	()	The Data Protection Law **does not expressly state the amounts** of penalties that will apply for breaches of the Law.
Implementation Period	Immediately, however a **two year grace period** was given.	)(	Executive regulations are due to be issued within six months of the date of issuance of the Law (i.e., by 20 March 2022). UAE companies will then have **6 months from the issuance of those executive regulations** to comply with the Law (although that period can be extended by the Cabinet).
Incident and Breach Response	Disclosure of incidents and data breaches without undue delay and within **72 hours** of the breach.	)(	The Controller shall, **immediately** upon becoming aware of such Breach, notify the Office of the Breach and the findings of the investigation.
Record of Processing Activities	Requires companies to create and maintain a record of processing activities. **RoPA is not required if an organization has less than 250 employees**, unless there's risk to the rights and freedom of data subjects/ involves sensitive data.	()	**Requires all companies** to create and maintain a more detailed record of processing activities, including details of persons authorized to access the data and the mechanisms for erasing, modifying or processing personal data.

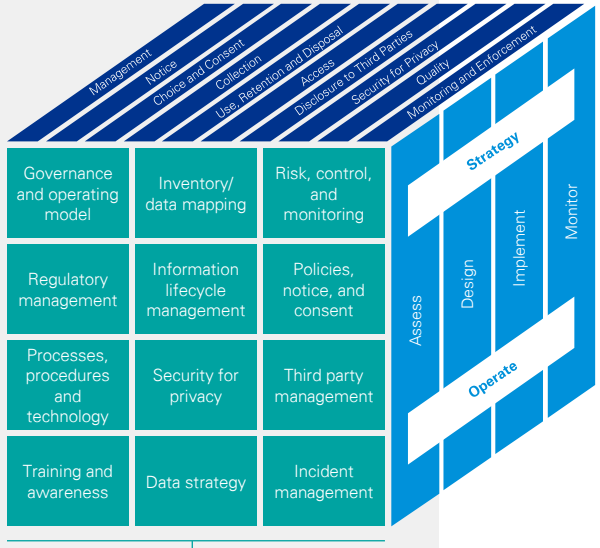
UAE Federal Data Protection Law vs GDPR?

Key: Similar: = Absent: X Broader: () Narrow:)(

Domain	GDPR	Key	UAE Federal Data Protection Law
Data Protection Impact Assessment	Data Protection Impact Assessments **are required**.	=	Assessment of the Impact of Protection of Personal Data **are required**.
Lawful basis for processing	**Six lawful basis** for processing personal data.	)(	**Five lawful basis for processing** - the Data Protection Law does not allow for processing on the basis of a controller's "legitimate interests".
Data Subject Rights	There are **eight** data subject rights under the GDPR.	)(	There are **six** data subject rights: 'right to be informed' seen within the GDPR is not defined in the UAE Law. The 'Right to Correct/ Delete' data are combined.
Rights Response Timeline	**1 month** with potential extension by **2 additional months**.	()	**No timeline** to respond to the data subject has been defined.
Marketing	Direct marketing permitted through **consent and legitimate interest**. Data subjects have the right to **object/ opt out**.	)(	Direct marketing permitted through **consent only**. Data subjects have the right to **object/ opt out**.
Cross Border Transfers	Permitted **under specific conditions** and if adequate levels of data protection are required.	)(	Permitted if the country or territory to which the Personal Data will be transferred **has legislations for protection of Personal Data**.

The UAE Federal Data Protection Law mapped to our KPMG framework

The figure below provides an overview of how these clusters of activities are mapped against the Federal Data Protection Law requirements.



Governance and operating model

Federal Data Protection Law Articles	
7	General obligations of the Controller
8	General obligations of the Processor
10	Designation of the data protection officer
12	Duties of the controller and processor towards the data protection officer

Risk, Control and Monitoring

Federal Data Protection Law Articles	
11	Tasks of the Data Protection Officer
21	Assessment of the impact of personal data protection

Information Lifecycle Management

Federal Data Protection Law Articles	
5	Controls of personal data processing
22	Transfer and share personal data outside the territory of the country where an adequate level of protection

Regulatory Management

Federal Data Protection Law Articles	
24	Filling complaints
25	Filing a complaint against the decisions of the office
26	Administrative sanctions and violations
27	Delegation

Policies, Notice, and Consent

Federal Data Protection Law Articles	
6	Conditions of consent to the processing of data
13	Right to obtain information
23	Cross-Border Transfer and Sharing of Personal Data In the Absence of Appropriate Protection Level

Processes, Procedures & Technology

Federal Data Protection Law Articles	
13	Right to obtain information
14	Right to personal data portability
15	Right to rectification and erasure of personal data
16	Right to restrict processing
17	Right to suspend processing
18	Right to processing and automated processing
13	Right to obtain information

Inventory/Data Mapping

Federal Data Protection Law Articles	
7.4	General obligations of the Controller
8.7	General obligations of the Processor

Security for Privacy

Federal Data Protection Law Articles	
20	Security of personal data information

Third Party Management

Federal Data Protection Law Articles	
7.5	General obligations of the Controller (Appointing a processor)
8	General obligations of the Processor

Incident Management

Federal Data Protection Law Articles	
9	Notification of data breaches

Training and Awareness

Federal Data Protection Law Articles
No articles defined in Federal Law.

Data strategy

Federal Data Protection Law Articles
No articles defined in Federal Law.

04

Implementing an effective data privacy program

Value of a privacy program

Minimized risk exposure and regulatory fines

With regulators imposing high fines for the infringement, regulatory compliance minimizes the chances of hefty financial penalties

Protected and enhanced organization and brand

UAE having millions of tourists per year means high visibility from around the world; a privacy program will help organizations in protecting its reputation by application of necessary controls to avoid data breaches or incidents.

Improved data security posture

Privacy and security continue to converge, a high level of data protection also means a high level of data security, an objective valued not only by customers, but every organization.

Increased trust, credibility and customer confidence

Data Privacy has a major impact on customer experience, a privacy program embeds privacy in the customer journey and ensures their data is protected along the way.

Key questions when implementing a privacy program...

Regulatory

— Do we know what regulations and data privacy laws apply to us?

— How do we respond to regulatory requests? Is here a process in place?

Privacy governance

— Who is responsible and accountable for data privacy with the company?

— Do we have a suitable governance structure in place?

Information security

— What security measures do we have in place to protect data?

— Do we have firewalls, anti-virus, anonymization encryption, password protection, access controls in place?

Data subject rights

— If a data subject wishes to delete or access their data, how will we locate their personal data? How to respond?

— Do we send unsolicited marketing emails? Do we have consent?

Breaches & incidents

— Do we have a breach/ incident management process or procedure?

— How do we inform data subject and conduct an investigation?

Retention and data mapping

— What personal data does the company retain and for how long?

— Have we documented our record of processing activities?

Vendors & suppliers

— Do we share personal data with any supplier or provide access to the data?

— Are their contracts in place with data protection clauses?

Employees & training

— Do our staff understand the risks associated with consumer data?

— Have we conducted training and awareness sessions?

Data privacy laws require that businesses take a holistic approach to privacy governance. UAE based organizations must be prepared to protect customer data through comprehensive privacy programs, with the goal of driving a culture of data privacy and protection throughout the company.

Implementing a data privacy program and appropriate controls

The KPMG Privacy Management Framework can be used to develop and implement a successful data privacy program.

The KPMG Privacy Management Framework is modular based on the OECD principles and Privacy Management Framework Elements and sub-components which define the foundation for privacy risk management activities that take place across an organization.

PRIVACY PRINCIPLES

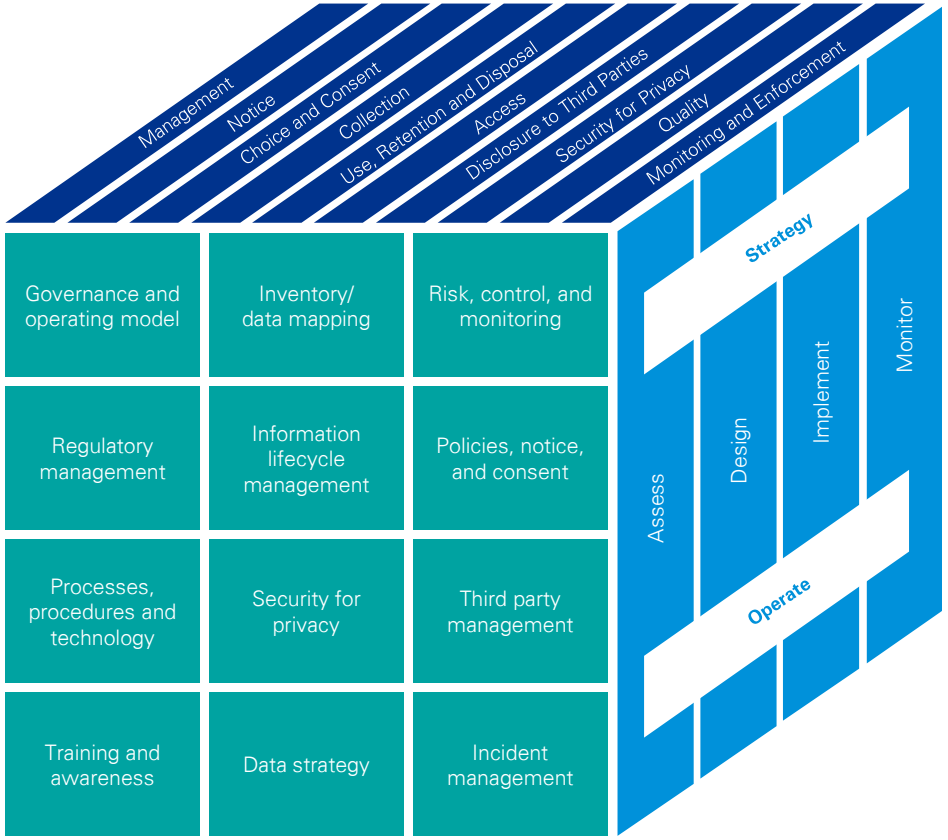
Privacy components are viewed against the internationally recognized 'Generally Accepted Privacy Principles', which provide the foundation for our privacy management framework

PRIVACY MANAGEMENT FRAMEWORK

Our framework elements are the distinct components that organizations employ to help ensure accountability with applicable privacy laws and regulations.

KPMG APPROACH

Our Privacy Service has been designed on the basis that organizations need tailored risk-based solutions to address their individual Privacy needs, risk appetite and future business strategy.



Sample end-to-end data privacy approach (at high level)

Plan

- ❑ Appoint a project manager.
- ❑ Establish a project plan
- ❑ Establish project status reporting
- ❑ Coordinate activities
- ❑ Plan and schedule meetings

1 week

Assess

- ❑ Understand your PII data landscape
- ❑ Identify applicable data privacy regulations
- ❑ Update our integrated controls framework.
- ❑ Conduct current state gap assessment
- ❑ Develop a remediation report.
- ❑ Develop a roadmap.
- ❑ Develop criteria for data privacy management tool selection (if applicable).

3 weeks

Design

- ❑ Develop or enhance the Data Privacy Framework.
- ❑ Establish privacy governance structure.
- ❑ Develop applicable policies, notices, procedure, SOPs, templates etc.
- ❑ Revise necessary contract and notice documentation.
- ❑ Design privacy management tool foundation layers (if applicable)

6 weeks

Implement

Wave 1

3.1 Discovery & Personal Data Inventory

- ❑ Discover PII
- ❑ Identify the key personal data processing activities.
- ❑ Populate the RoPA

3.2 Data Protection Impact Assessment (DPIA)

- ❑ Implement DPIA framework.
- ❑ Identify the high-risk processes
- ❑ conduct DPIAs where applicable.

Wave 2

3.3 Data subject rights

- ❑ Implement data subject rights processes and procedures.
- ❑ Develop templates.
- ❑ Roll out the controls to manage the requests.
- ❑ Conduct test runs.

3.4 Consent Management

- ❑ Identify touchpoints where data subjects make informed choices.
- ❑ Implement consent mechanism(s) where applicable.

Wave 3

3.5 Third Party Management

- ❑ Implement Third Party risk assessment process.
- ❑ Conduct due diligence on third parties.
- ❑ Evaluate and report on privacy risks.

3.6 Breaches & Incidents

- ❑ Implement breach management process.
- ❑ Conduct test runs.
- ❑ Remediate gaps/ issues.

12 weeks

Monitor & Train

- ❑ Develop checklists, compliance dashboards, templates as required to monitor the progress and compliance.
- ❑ Horizon scanning.
- ❑ Conduct awareness sessions with employees.
- ❑ Conduct role-based advance training for individuals in higher risk roles.

On-going

Project Management, Quality Assurance, Organizational Change Management

KPMG's global data privacy footprint

Global experts in data protection

Our global team consists of **500+ trained data protection resources** that are also members of IAPP. Our team also hold the IAPP's certifications as seen below:

iapp

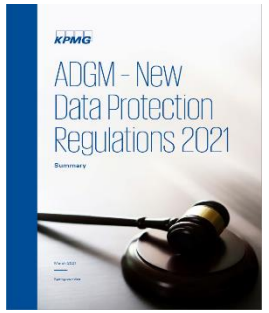
KPMG Diamond membership with the International Association of Privacy Professionals (IAPP).

CIPT CIPP CIPM CDPSE CSP CHFI CISM CISA

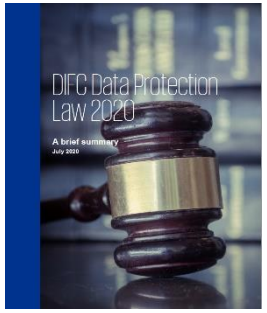
Our thought leadership

Through our Global Privacy Advisory network, KPMG regularly publishes Privacy thought leadership and continuously enhances its offerings.

GDPR: Privacy as a Way of Life



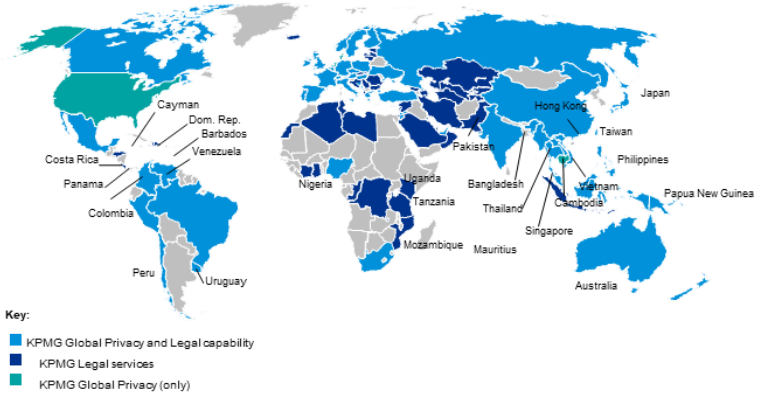
ADGM – New Data Protection Regulations 2021



The DIFC Data Protection Law 2021

Global office locations

Our regional data protection Center of Excellence is based in the UAE with certified and experienced professionals.



Our global technology partnerships

Through our Global ecosystem of technology partners, we deliver end to end privacy solutions.

An innovative ecosystem of data protection and privacy technology partners

Microsoft Forcepoint BigID McAfee OneTrust GETVISIBILITY DIGITALGUARDIAN DATAGUISE

Our global alliance with OneTrust

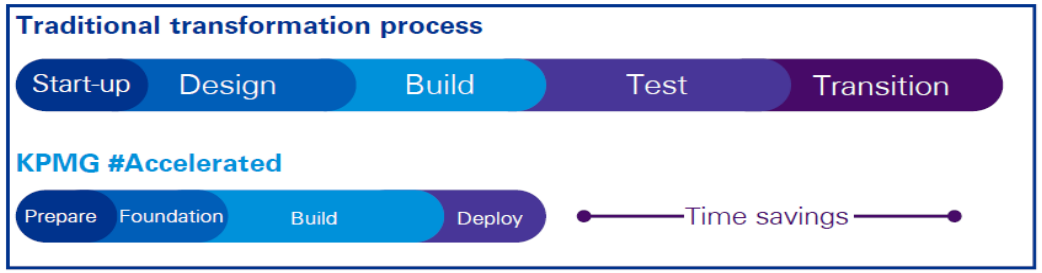
Competitive advantages of our global alliance and our unique capabilities

KPMG — OneTrust PRIVACY, SECURITY & GOVERNANCE

— KPMG's **Accelerated Privacy** solution and methodology helps clients to accelerate their privacy compliance transformation projects.

— We have a standardised **OneTrust** configuration ready for your validation.

— This means we can **accelerate delivery at a lower risk**, and with a higher degree of certainty and success with a **reduced time for implementation.**



"Accelerate your Privacy program with a ready to use pre-configured technology platform leveraging KPMG best practices, instead of starting from scratch."

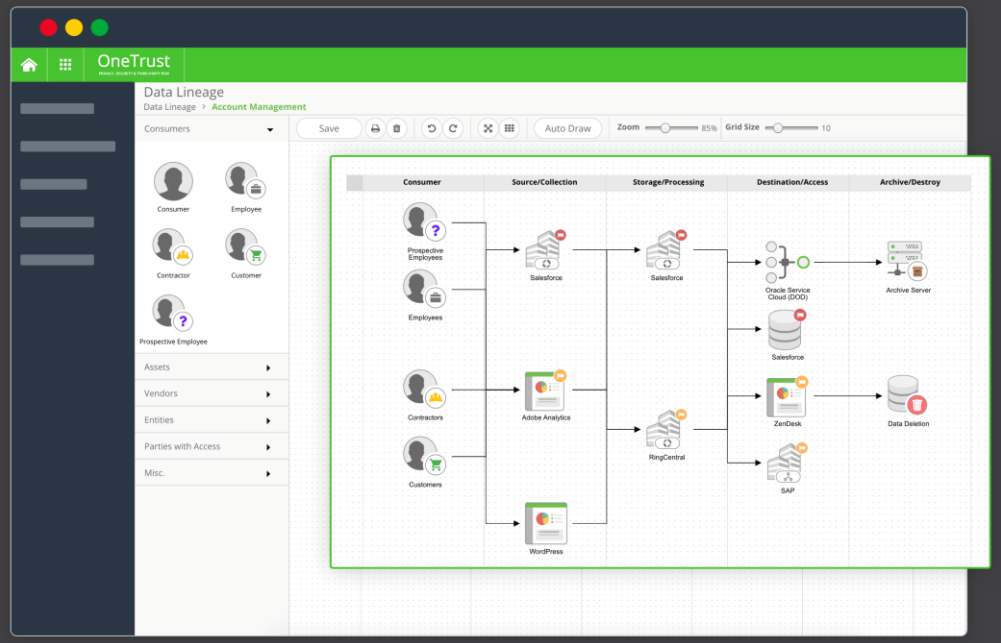
05

How to automate privacy and fast-track compliance

Trusted by 7,500 Organizations, Both Big and Small

OneTrust Privacy

PRIVACY MANAGEMENT SOFTWARE



DATAGUIDANCE INTELLIGENCE

Same Day Support for Regulatory Updates from 40 In-House Legal Experts and 800 Expert Contributors

LONG-TERM TECHNOLOGY PARTNER

Pioneering Privacy Technology with 135 Patents and Monthly Product Releases by the Largest R&D Team

QUALIFIED TEAM OF PRIVACY PROS

World's Largest Install Base of IAPP CIPPs with 400+ Certified Privacy Professionals

LARGEST PRIVACY COMMUNITY

Don't Go At It Alone – Share Best Practices Online, In 125 Local Chapters

ONETRUST ATHENA™ AI

AI & Robotic Automation to Operationalize Regulatory Requirements and Streamline Common Processes

OneTrust
PRIVACY, SECURITY & GOVERNANCE

BUILT FOR:
Privacy, Security, IT & Legal Teams

BUILT FOR:
Security, Data, Analytics & Technology Teams

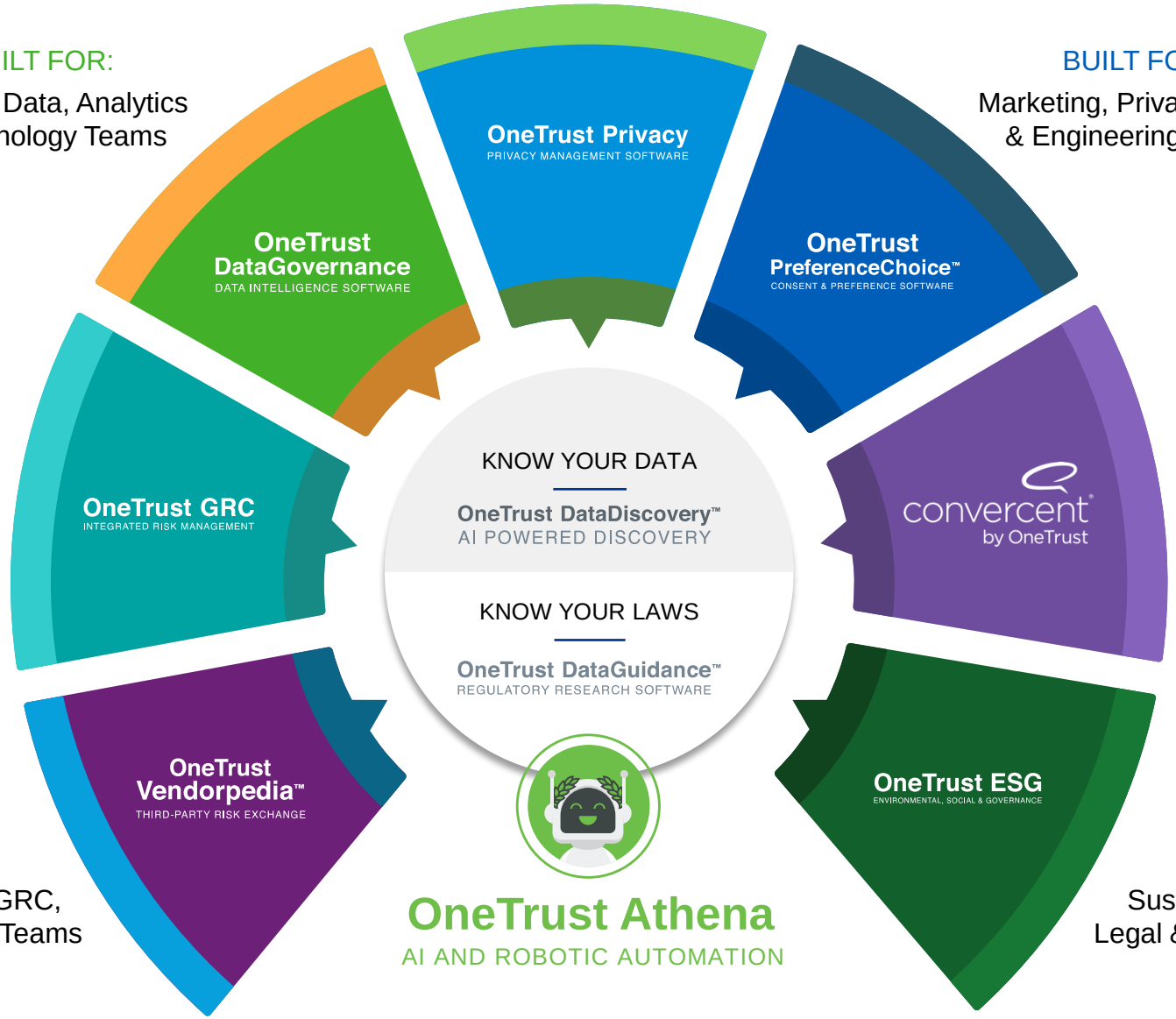
BUILT FOR:
Marketing, Privacy, Media & Engineering Teams

BUILT FOR:
Infosec, Audit, Risk & Compliance Teams

BUILT FOR:
Ethics, Compliance, HR & Legal Teams

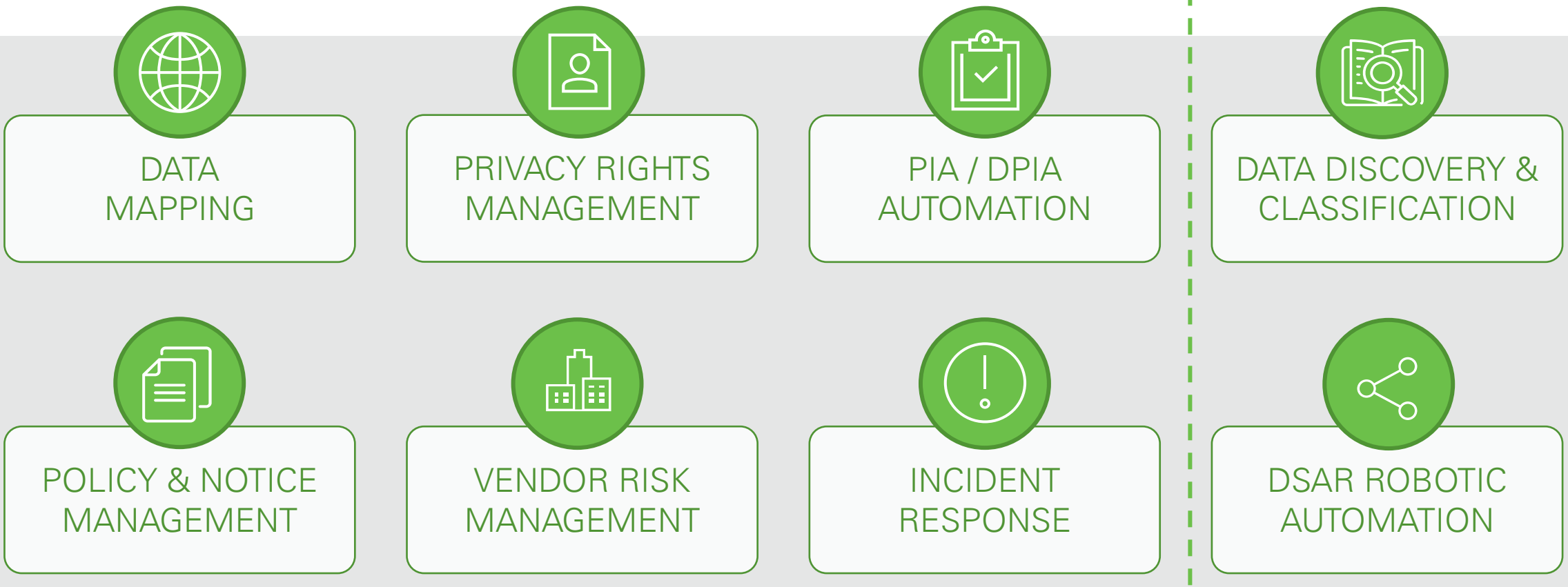
BUILT FOR:
Infosec, Privacy, GRC, Sourcing & Vendor Teams

BUILT FOR:
Sustainability, Finance, Legal & Procurement Teams



Make Trust a Competitive Advantage with **OneTrust**

A Central View Into Your Privacy Program



OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust

REPORTS

- Dashboards
- Reports
- Schedules

Dashboards

Dashboards > DPO Dashboard

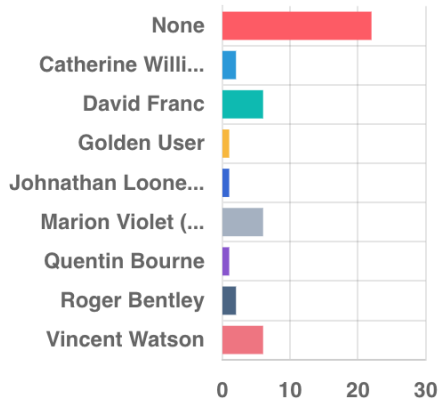
Edit

SAR's Due this week

7

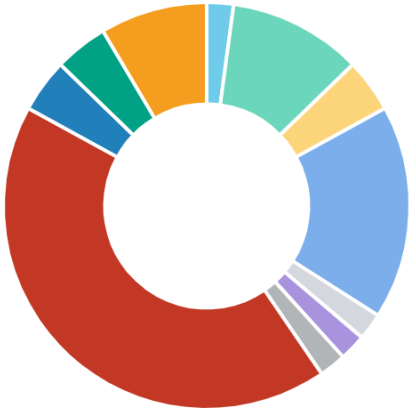
Requests

DSAR's pending completion by approver

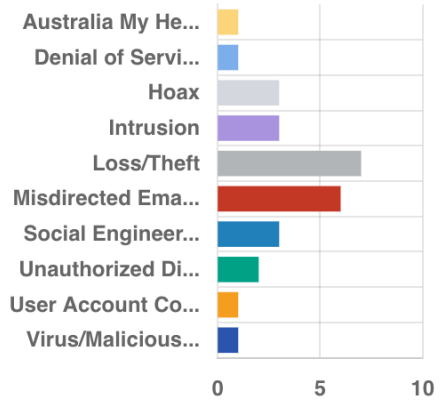


Rejected Requests Last 90 Days

Requests By Type



Open Incidents by Type

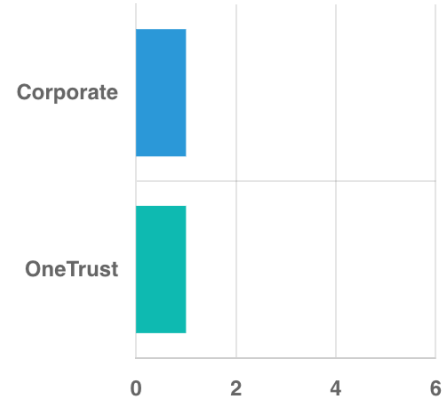


Incidents Requiring Notification

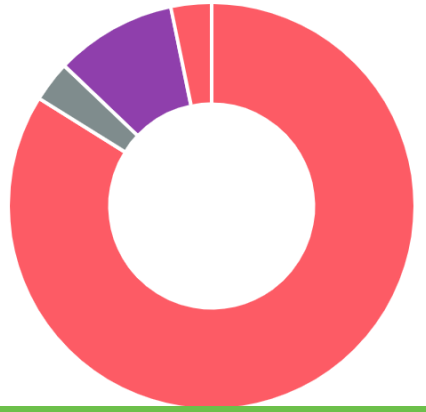
31

Incidents

Incidents Resolved Last Week



Incidents by Severity



DPO dashboards for central, real-time view into your privacy program

OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust

CONSUMER REQUESTS

- Dashboard
- Reports
- Requests
- Subtasks
- Setup
- Settings

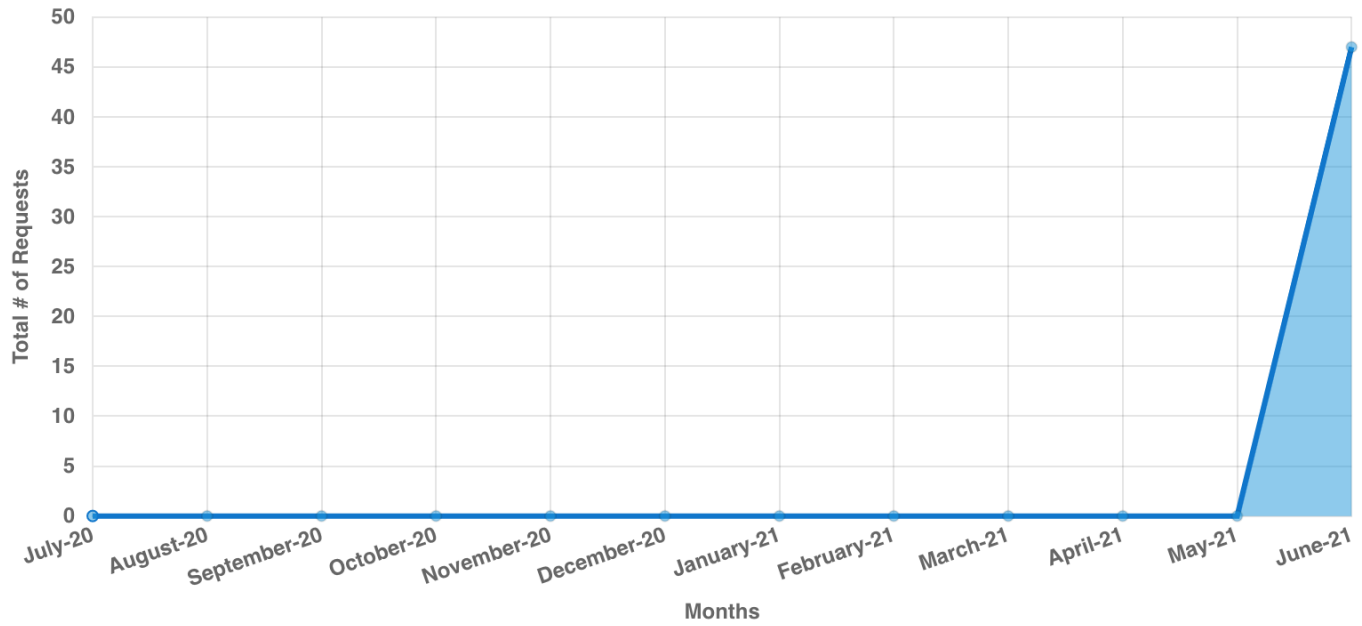
Consumer Request Dashboard

New Dashboards

Summary Metrics

47	4
Requests Received	Requests Completed
0.04	$375
Days Average Time to Complete	USD Average Cost

Requests By Date

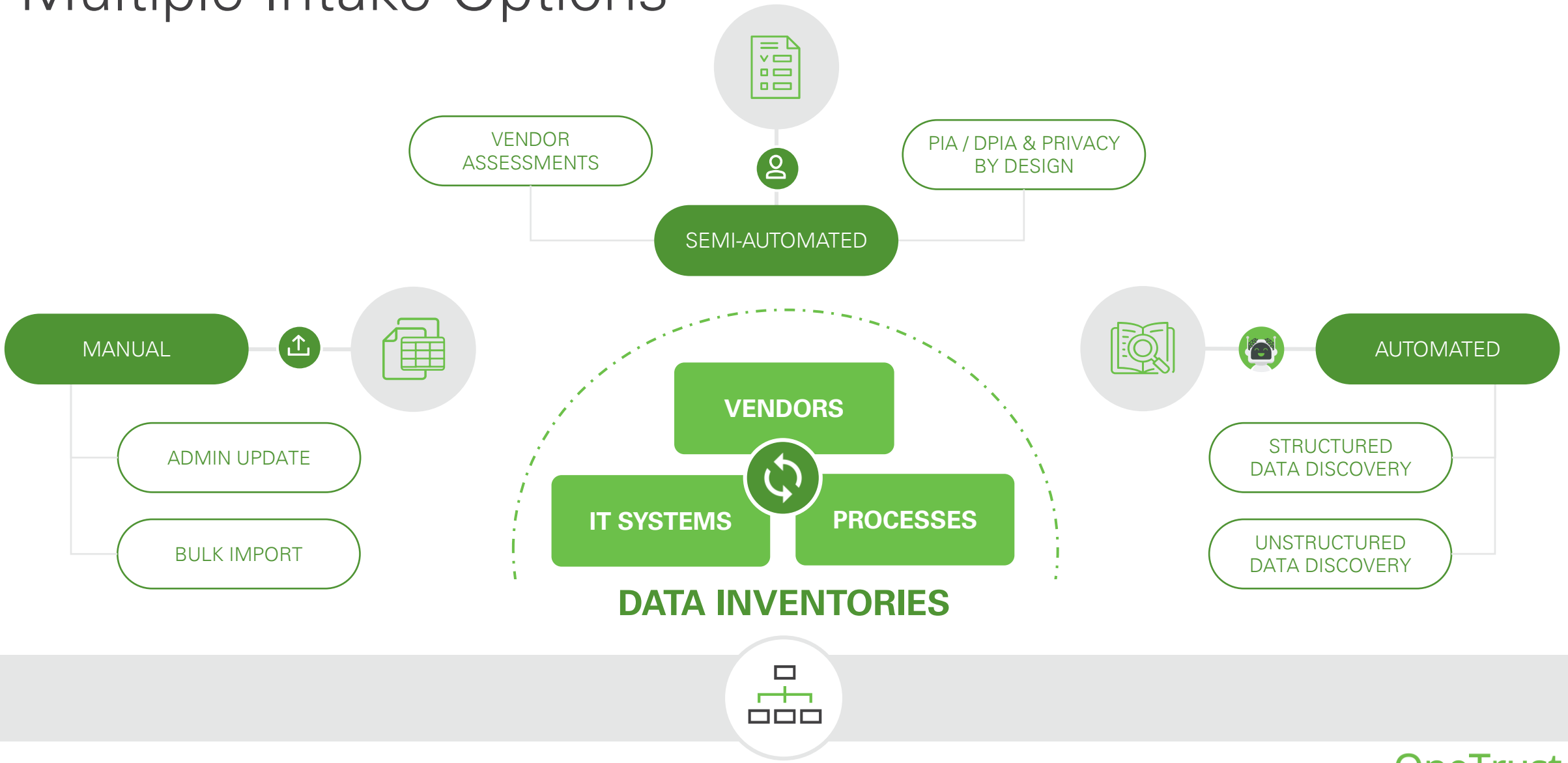


Requests By Country

Select View: World View

Monitor incoming privacy rights (DSAR) requests

Multiple Intake Options



OneTrust
PRIVACY, SECURITY & GOVERNANCE

DATA MAPPING
Dashboard
Assessments
Risk Register
Inventory
Assets
Processing Activities
Entities
Vendors
Reporting
Asset Map
Cross-Border
Data Lineage
Reports
Setup
Data Mapping Settings

Cross-Border

Filter by Processing Activity: All

Visualize cross border transfers of data and assess that valid transfer mechanisms are in place

INCIDENT RESPONSE
Dashboard
Incident Register
Databreachpedia
Templates
Setup
Workflows & Rules
Incident Types
Attribute Manager

Incident Details

Incident Register > 30 - 2019-10-23

Analyze

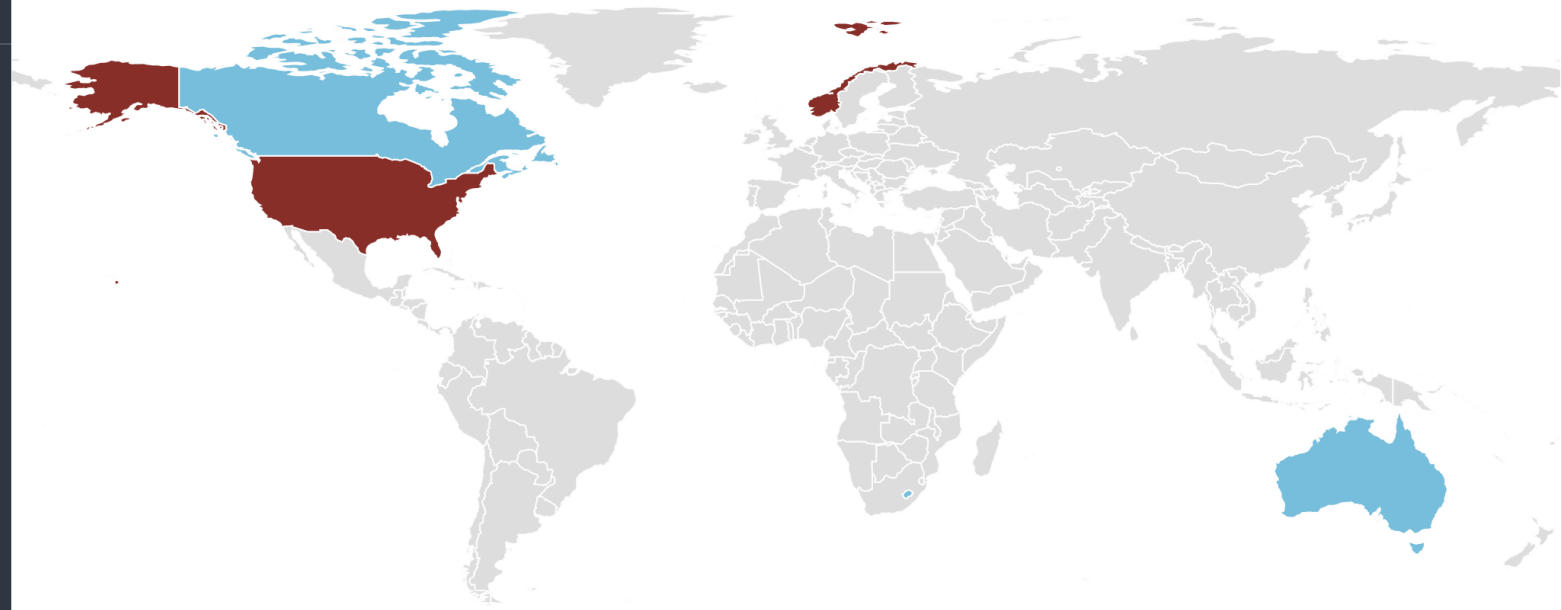
Incident Guidance Checklist | Change Workflow

NEW | INVESTIGATE | REMEDIATE | ANALYZE | NOTIFY | COMPLETE

Advance

Summary | Details | Assessments | **Jurisdictions** | More

Assess Jurisdictions | Manage



Open Subtasks

- Notify the Primary Federal Regulator/Consu...
- Notify the Credit Reporting Agencies (CRAs) (...
- Notify the Primary Federal Regulator/Board ...
- Notify the Primary Federal Regulator/ Nation...

View All Subtasks

Assessments

- Incident Guidance Assessment

View All Assessments

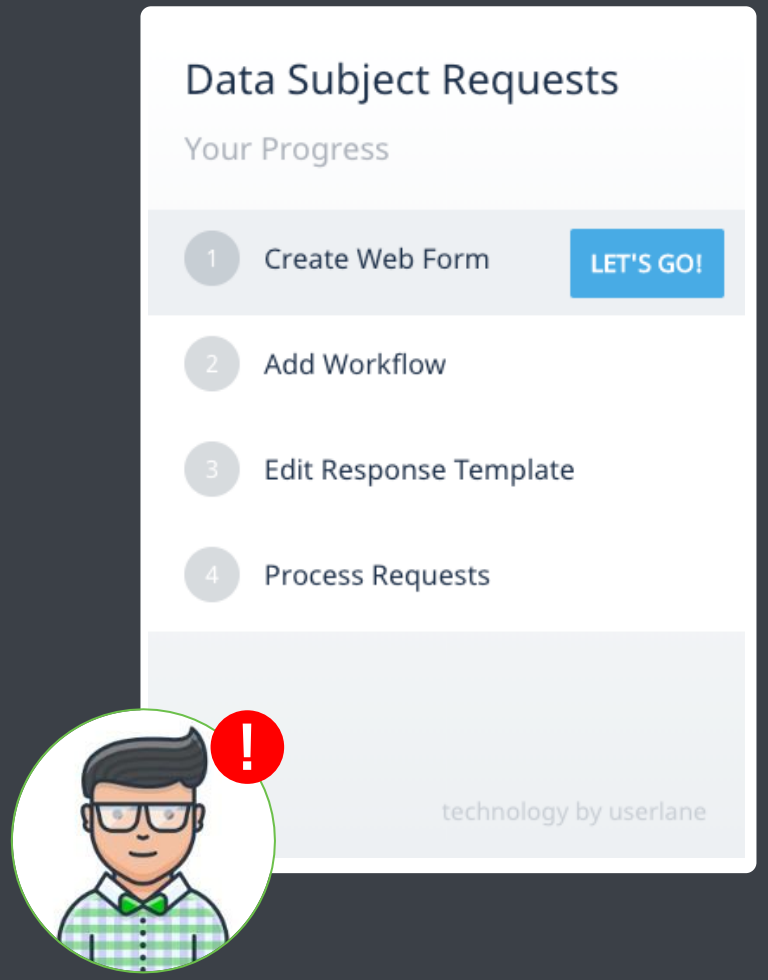
Attachments

- pdf-0154_data-breach-response-guide-for-bus...
- Privacy Breach Investigation Procedure 10.28...

View All Attachments

Intake and action incidents through configurable workflows and notification guidance from OneTrust Athena AI

Simple to Setup with Built-In Guidance



IN-PRODUCT GUIDANCE

Launch anywhere, any time, for any product

Step-by-step guide to get up and running

Highlights key features & settings and how to use them

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Thank you!

Timothy Wood
Engagement Partner
Digital and Innovation - Cyber
KPMG Lower Gulf Limited
+971 56 409 6842
timothywood@kpmg.com

Maliha Rashid
Engagement Director
Digital & Innovation - Cyber
KPMG Lower Gulf Limited
+971 50 608 2013
mrashid5@kpmg.com

www.kpmg.com/ae | www.kpmg.com/om

Follow us on:

@kpmg_lowergulf