protiviti®
Face the Future with Confidence

THE GENERAL DATA PROTECTION REGULATION (GDPR) JOURNEY

TODAY'S PRESENTER

Jeff Sanchez

Managing Director, Security and Privacy Leader

Protiviti

AGENDA

- GDPR Overview
- “Personal Data” as defined by GDPR
- Key Requirements
- GDPR Scenario
- Practical Guidance - Building a GDPR Compliance Plan

GDPR OVERVIEW

OVERVIEW

What is GDPR?	• General Data Protection Regulation • Replaces local EU Data Protection Directive implementations (e.g., in UK the “Data Protection Act”) • **Starts on May 25, 2018**
Who is Subject?	• **All organizations that collect and process personal data of EU data subjects** – regardless of size • No longer applies only to organizations with an office the EU - **is borderless** • **Applies to data processors** - not just data controllers
What are the Penalties?	• Up to 20M € or 4% of organization’s annual global turnover, whichever is higher (board attention is now guaranteed) • Data subjects can claim **compensation for damages** from breaches to their personal data

protiviti

GDPR PERSONAL DATA

PERSONAL DATA

GDPR Rules

This definition is important because EU data protection law expands the traditional definition of “personal data”. Information that previously did not fall within the traditional definition of "personal data" is now subject to EU data protection law.

What is Personal Data?

Personal Data is defined as:

- Any information relating to an identified or identifiable natural person, “data subject”.
- An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as name, address, online identifiers, location identifiers, financial data, healthcare data, etc.

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 1

Vehicle Identification Number (VIN)

protiviti

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 1

Vehicle Identification Number (VIN)

Yes

"…the vehicle identification is directly related to the identity of the owner of the car who is in several cases identical with the driver"

Opinion of the EDPS on the proposal for a Regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall system and amending Directive 2007/46/EC

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 2

Employee ID number

protiviti

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 2

Employee ID number

Yes

"…Accordingly, in the business context, a photo of someone on an identification badge or on a video monitor is "personal data," as is a listing of employee salaries designated either by employee name or **some identification number** (company ID number, social security system/tax ID number)

Proskauer on Int'l Litigation and Arbitration

protiviti

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 3

Meal Preference on Commercial Air Travel

protiviti

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 3

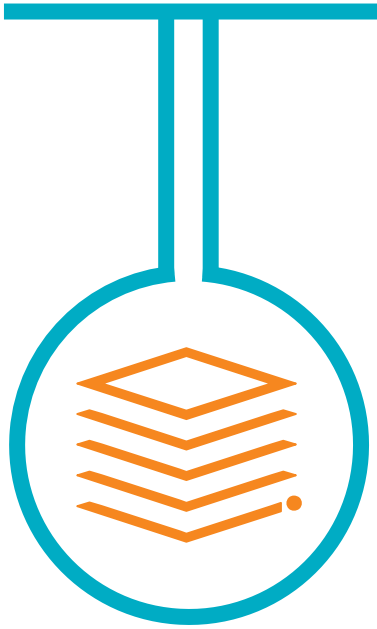
Meal Preference on Commercial Air Travel

No

Not listed as one of the 19 elements that makes up personal data on Annex I of DIRECTIVE (EU) 2016/681:

DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

PERSONAL DATA ON ANNEX 1 EU



- PNR record locator
- Date of reservation/issue of ticket
- Date of travel
- Name
- Address/Contact info
- All forms of payment
- Complete itinerary
- Frequent flyer info
- Travel Agent info
- Travel status of passenger
- Split PNR info.
- General remarks
- Ticketing field info
- Seat number
- Code share
- All baggage info
- Number and order names
- Advance info
- All historical changes to the PNR listed in the above 18.

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 4

Photo (assume no other information)

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 4

Photo (assume no other information)

Yes

Implied by Rec. 51 of the GDPR:

"The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person."

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 5

Opinions about others (typically in employment)

protiviti

IS THIS PERSONAL DATA UNDER THE GDPR?

Question 5

Opinions about others (typically in employment)

Yes

"The definition [of personal data] also specifically includes opinions about the individual, or what is intended for them."

U.K. Information Commissioners Office, Key definitions of the Data Protection Act

PERSONAL DATA DEFINITION

Any information

relating to an

identified or **identifiable** ***natural person*** (***"data subject"***)

who is and/or can be identified,

directly or **indirectly**

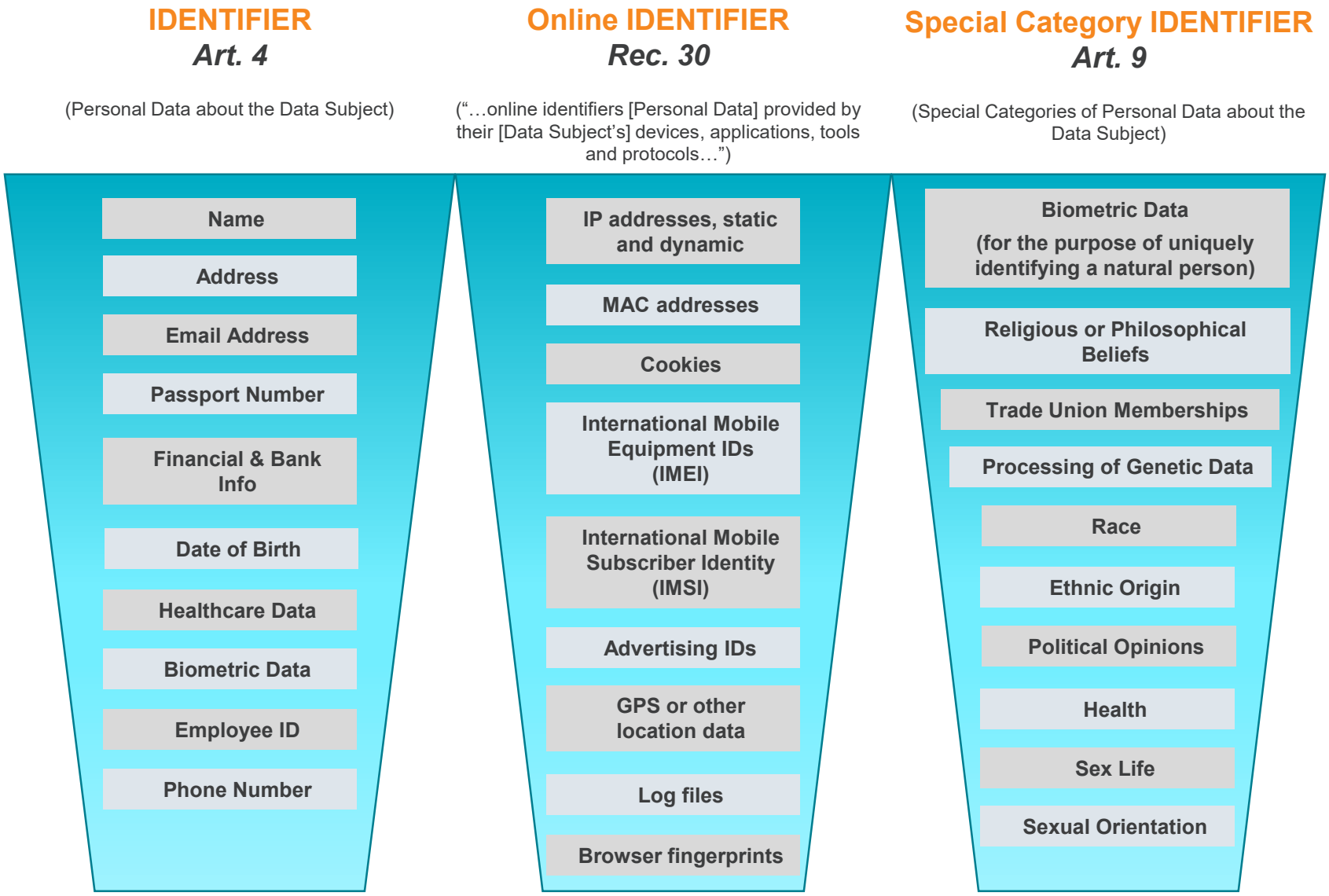
in particular by reference to

one or more **identifiers** (***"types of subject data"***)

such as

- **Personal Data – Art. 4**
- **Online Identifiers – Rec. 30**
- **Special Category Personal Data – Art. 9**

3 BUCKET TYPES OF IDENTIFIERS FOR PERSONAL DATA



protiviti

BUILDING A GDPR COMPLIANCE PLAN

THE REGULATION

protiviti

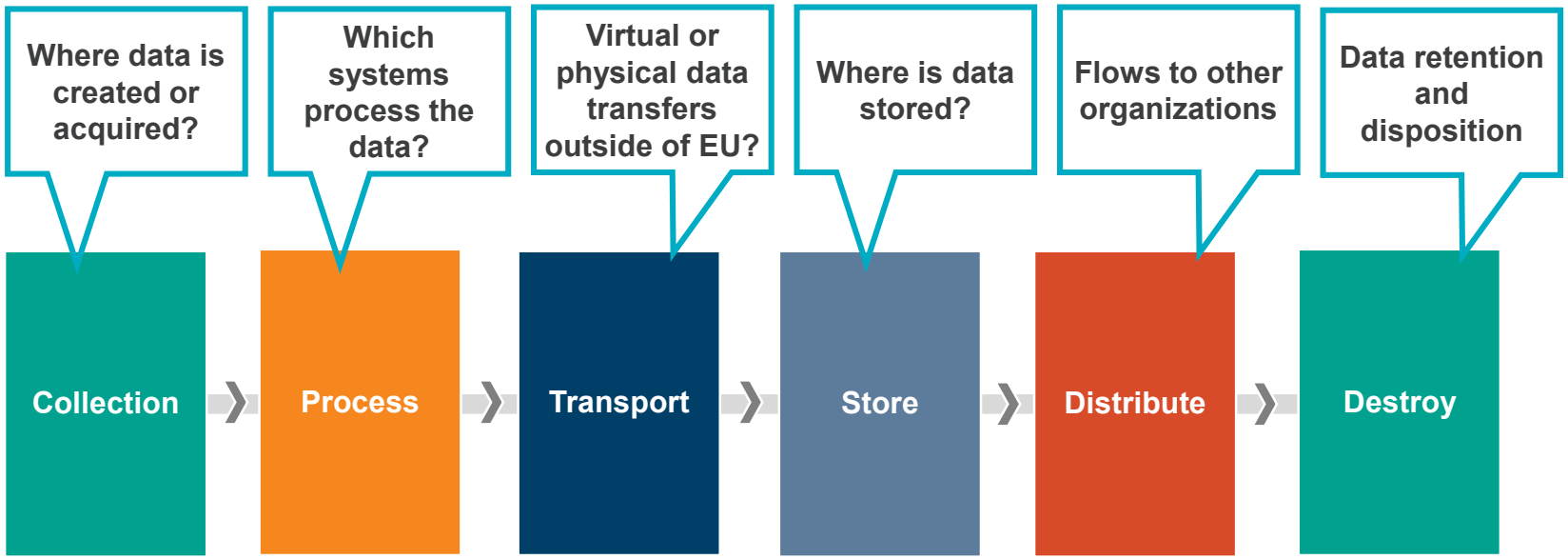
GDPR - APPROACH TO COMPLIANCE

Discovery & Inventory	Gap Analysis	Compliance Remediation	Ongoing Compliance
• Inventory of EU data subjects' personal data, including classification level, data controller, processor and exchanges • Formal inventory of processing activities	• Assess data collection, processing, storage and protection measures, assignment of a DPO, transfers to 3rd parties, risk assessment practices and security policies	• Obtain executive management support and funding • Establish compliance program structure and governance • Identify compliance strategies • Implement remediation plans	• Testing and validation • Implementation of monitoring tools and processes
Identify high risk areas to ensure a focused approach.	Determine exposure and prioritize compliance activities	Implement changes to achieve compliance	Provide evidence of accountability & compliance

Phase duration and level of effort is highly dependent on personal data processed, the size and scope of your environment and process complexity and maturity.

protiviti

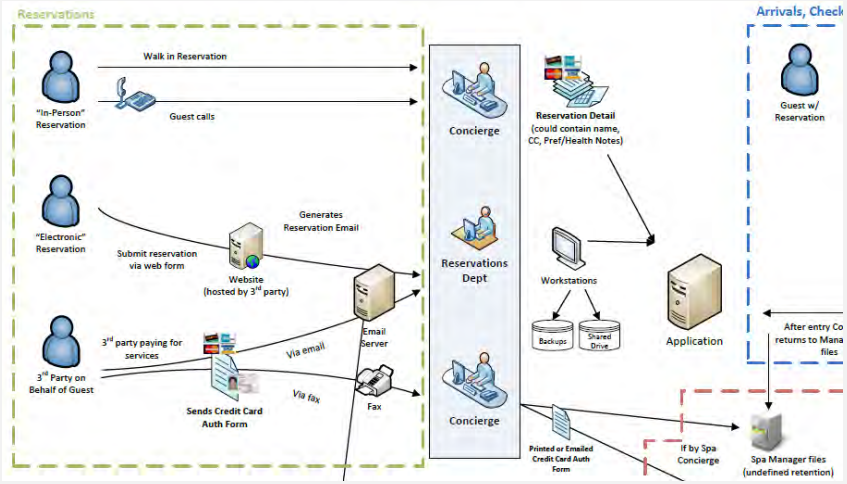
Data Inventory – Applications and Third Parties



In-scope applications and third parties should be prioritized:

- **High Risk** – High probability that a data breach can occur
- **Medium Risk** – Moderate probability that a data breach may occur
- **Low Risk** – Low probability that a data breach may occur

protiviti



	Name	Address	Date of Birth	Email Address	Phone Number	Home address	Bank Account Details	UK National Insurance Number	Job title	Past Employer References	Internet Usage / Browsing History	Offences / Incidences
Customers	●	●	●	●	●	●			●		●	●
Employees	●	●	●	●	●		●	●		●	●	

● Data originally collected in the US

● Data originally collected in the UK

protiviti

GDPR requirements should be evaluated to identify gaps and develop remediation plans:

- Legal Basis for Processing
- Consent
- Privacy Notice
- Data Subject Rights
- Data Security
- Records of Processing Activity
- Third Party Due Diligence
- Privacy by Design and by Default
- Breach Notification
- Data Protection Impact Assessment
- Data Protection Officer
- Cross-border Data Transfers

Determine Risk:

- High
- Medium
- Low

Responsible Parties:

- Legal
- IT
- Information Security
- Business

protiviti

COMMON GDPR GAPS

01 **Data Privacy by Design** – Poor data mapping / lack of priority in design

02 **Rights of Data Subjects** – CRM systems may need major redesign

03 **Third Party Management** – Data processors, responsibility, contracts

04 **Conditions for Consent** – Using historical data may be a challenge

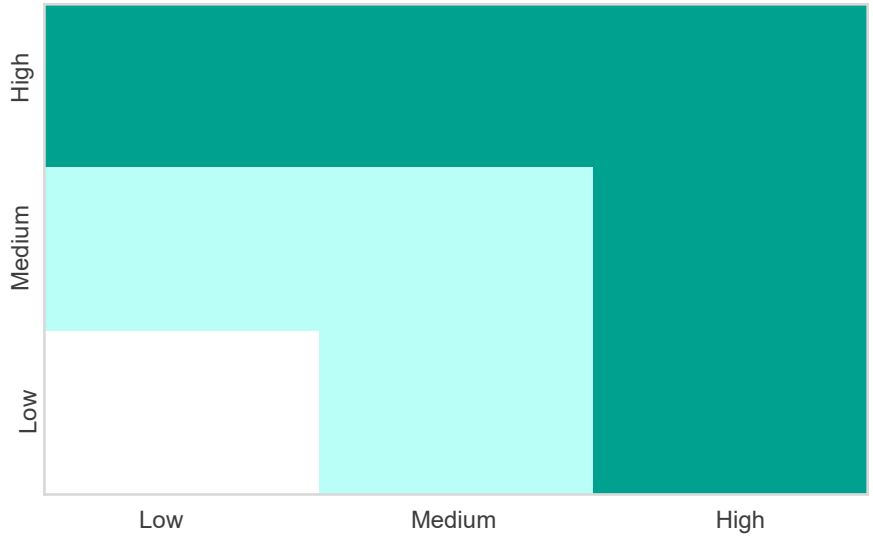
05 Accountability (legal, compliance, IT, HR, customer service)

06 **Security of Processing** – Formalizing data processing, use of encryption

07 **Data Breach Reporting and Communication** – Process enhancement

protiviti

Heat map Example



Requirements

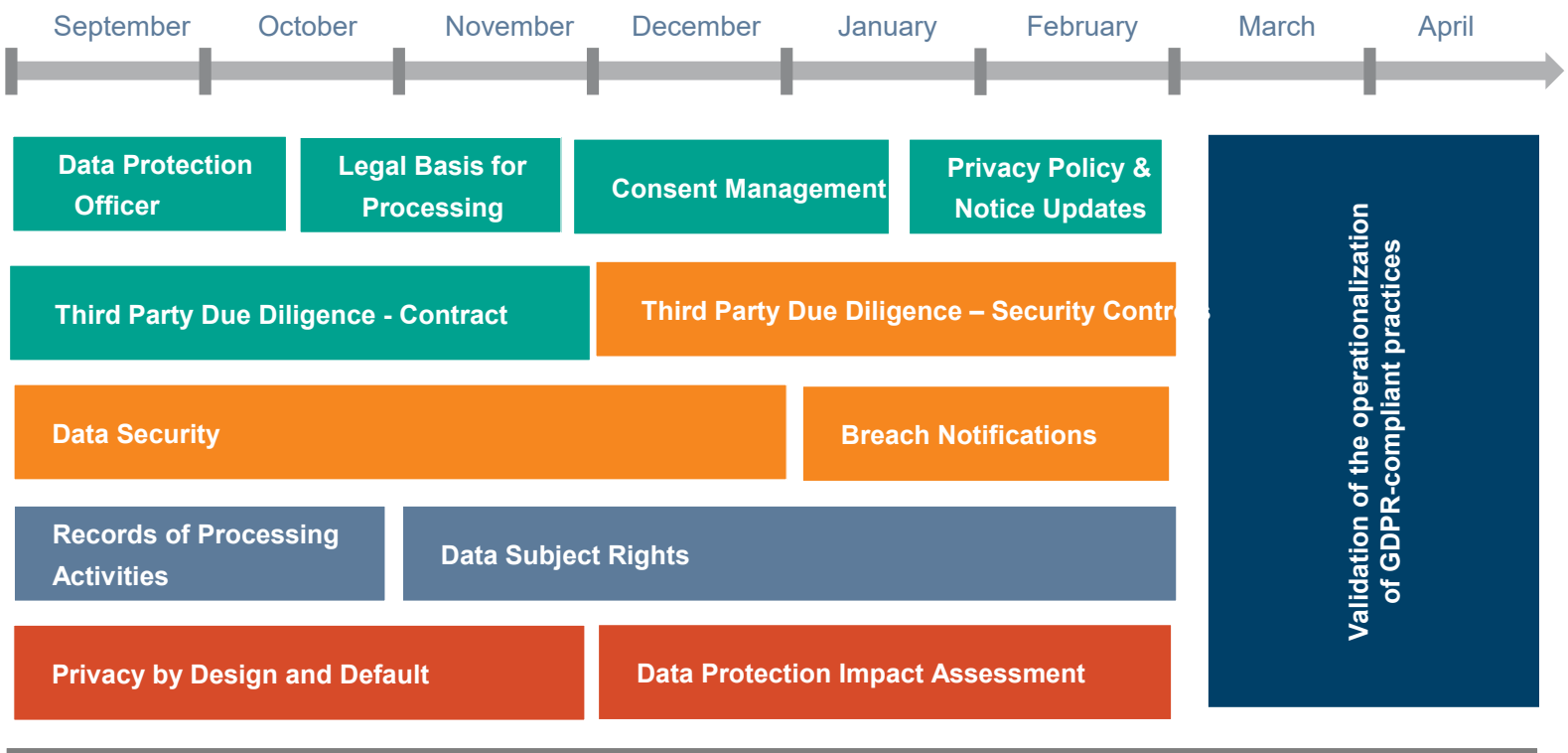
1. Legal Basis for Processing
2. Consent
3. Privacy Notice
4. Data Subject Rights
5. Privacy by Design and by Default
6. Third Party Due Diligence
7. Records of Processing Activity
8. Data Security
9. Breach Notification
10. Data Protection Impact Assessment
11. Data Protection Officer
12. Cross-border Data Transfers

Determine your Criteria

- **Plot:** Effort, Impact, Duration, Cost, etc
- **Risk**: High, Medium, Low

protiviti

ILLUSTRATIVE COMPLIANCE ROADMAP



protiviti

Data Inventory Maintenance

- Assign roles and responsibilities to keep it accurate
- Establish a change management process to keep it accurate
- Consider data inventory and data mining tools to keep it accurate

Documentation & Monitoring

- Assign roles and responsibilities to monitor compliance
- Control Documentation / Management
- Policy Management
- Training

GDPR WILL REQUIRE ONGOING VALIDATION AND COMPLIANCE MANAGEMENT PROCESSES

ROLES AND RESPONSIBILITIES ON GDPR PROJECTS

ROLES AND RESPONSIBILITIES

STEERING COMMITTEE

1. Overall strategic direction for how the organization will manage GDPR **data.**
2. Ownership of the **data classification** scheme and rules for each classification level.
3. Defining and approving Data Owners.
4. Alignment of data management with overall business strategy and goals.
5. Provide oversight for activities that impact compliance.

protiviti

IT/SECURITY

- Facilitates implementation of security controls (systems and physical) to address privacy concerns.
- Provides technical expertise on security concepts.
- Gathers, analyzes, and reports on effectiveness of data privacy program.
- Enforces compliance with data privacy policy and standards.
- Oversees the annual risk assessment process.
- Coordinates the development and implementation of information security and data privacy awareness training.
- Coordinates a response to actual or suspected breaches in the confidentiality, integrity, or availability of SPI.

INTERNAL AUDIT

- Oversee that the IA plan accounts for data protection assessment activities.
- Review whether or not data protection is in-scope for cross audit considerations.
- Assess whether or not the organization is ready for GDPR compliance.
- Provides expertise on risk, compliance, and ethics.
- Provides insight on the auditability of privacy controls.
- Raise privacy issues from within audit.
- Provides guidance on aligning privacy with internal policies.
- Assist with compliance and policy enforcement including investigation of issues.
- Ensure transparency of the overall data privacy program.

LEGAL

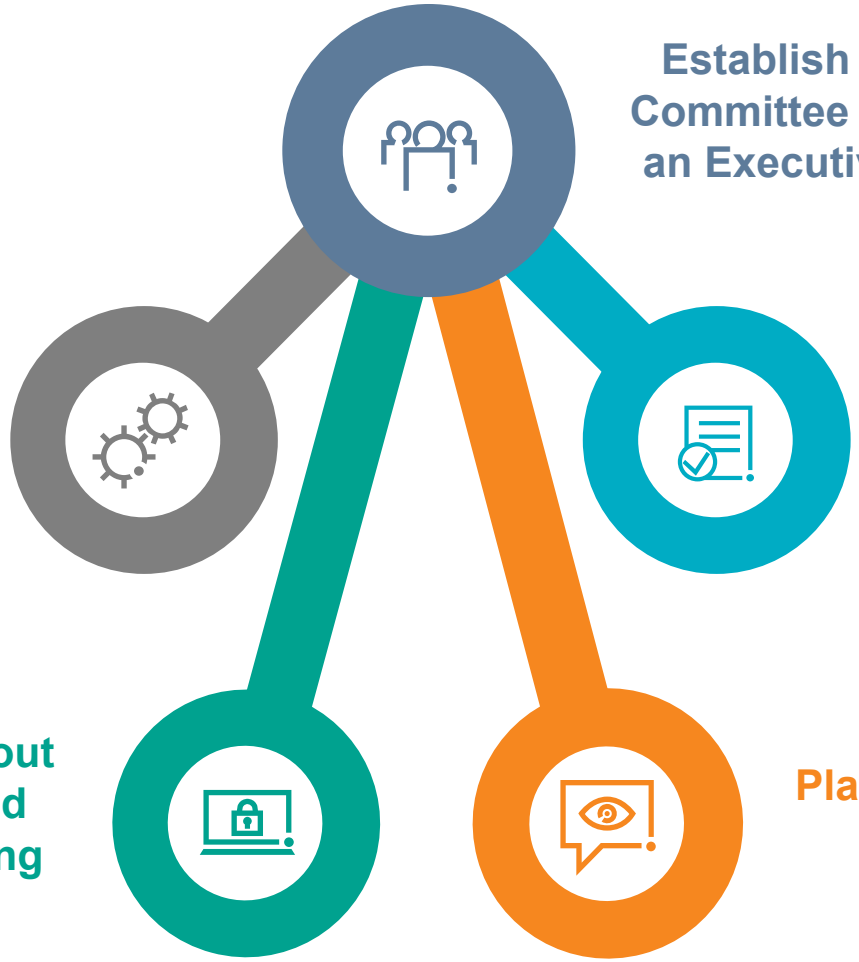
- Communicates strategic direction of privacy.
- Provide insight and guidance on the requirements.
- Facilitates execution of the privacy program objectives.
- Assist with relevant policy and strategies.
- Provides **guidance** on interpreting applicable laws and regulations.
- **Identifying** new laws and regulations, updates and changes to existing laws and regulations, and their impact to privacy strategy.
- Ensuring data privacy strategy addresses all applicable regulations **(compliance)**.
- Contact for law enforcement, state and federal agencies.

OTHER

- Communication to respective parties about new technologies or data elements that may introduce impact to compliance efforts.
- Providing assistance with relevant risk assessments.
- Support various departments with compliance needs.
- Identity changes in business that impact privacy.
- Provide appropriate liaison between departments to ensure appropriate coverage of compliance needs.

protiviti

FINAL THOUGHTS



Establish a Steering Committee and identify an Executive Sponsor

Understand where your data lives

Formalize your Path to Compliance

Collaborate throughout the organization and integrate with existing processes

Plan your story to tell

protiviti

Q & A

APPENDIX

EXAMPLES OF HOW TO RUN AFOUL OF DATA PROTECTION AUTHORITIES

(MASS) PERSONAL DATA COLLECTION WITHOUT PERMISSION

Offender	Facebook; Facebook Ireland
DPA	CNIL (France)

Facts

- FB amended their privacy policy in 2015…
- CNIL (and others) conducted an audit, and found:
  - "…FACEBOOK proceeded to a massive compilation of personal data of Internet users in order to display targeted advertising.
  - "…FACEBOOK collected data on browsing activity of internet users on third-party websites, via the "datr" cookie, without their knowledge."

(MASS) PERSONAL DATA COLLECTION WITHOUT PERMISSION

In Particular

- Did not provide direct information to internet users concerning their rights and the use that will be made of their data.
- Collected sensitive data of the users without obtaining their explicit consent.
- By using the web browser settings, did not allow users to validly oppose to cookies placed on their terminal equipment
- Did not demonstrate the need to retain the entirety of IP addresses of users all along the life of their account.

FB was notified, but returned “unsatisfactory responses”

Fine	€150,000

NOT VETTING SUB-CONTRACTORS

Offender	HCA International Ltd.
DPA	ICO (U.K.)

Facts

- The London hospital is part of a worldwide network of private health care facilities offering a range of services including fertility treatment.
- In April 2015 a patient found that transcripts of interviews with IVF patients could be freely accessed by searching online.
- Audio records sent to India for transcription, then sent back to London.
- However, audio files and transcripts stored on an unsecured server in India.

NOT VETTING SUB-CONTRACTORS

The ICO

- “What makes this case even worse is that we know the company is aware of its data protection obligations and already has appropriate safeguards in place in other areas of its business. **The situation could have been avoided entirely if HCA International had taken the time to check up on the methods used by the contract company.”**

Fine **£200,000**

protiviti

NO DUE DILIGENCE ON MERGERS & ACQUISITIONS

Offender	TalkTalk
DPA	ICO

Facts

- Attack took place between 15 and 21 October 2015.
- Attacker accessed personal data of 156,959 customers including names address, DOB, phone numbers and email
- In 15,656 cases, the attacker also had access to bank account details and sort codes.
- In 2009, TalkTalk bought ISP Tiscali, but did not conduct a vulnerability assessment on the company's IT infrastructure
- TT was unaware that a web page linked to a customer database
- Attackers used a SQL injection attack to obtain the data

NOT VETTING SUB-CONTRACTORS

Information Commissioner Elizabeth Denham:

- "In spite of its expertise and resources, when it came to the basic principles of cyber-security, **TalkTalk was found wanting**.
- **"Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue**. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers."

Fine **£400,000**

FACILITATE MONEY LAUNDERING WITH CUSTOMERS' IDENTITY

Offender	**UK-based Sigue Global Service Limited plus four agent companies in Italy**
DPA	**Il Garante per la protezione dei dati personali**

Facts

- Sigue used the names of its customers to make more than €1B in money remittances to China.
- Broke up the transfers among many customers in order to evade money laundering controls
- Attribution of the money transfers to persons who had not provided consent was a violation of the Italian Data Protection Code.

FACILITATE MONEY LAUNDERING WITH CUSTOMERS' IDENTITY

Fine

€5,880,000 on Sigue

Fines of €1,590,000, €1,430,000, €1,260,000 and €850,000, respectively, on the other four companies,

Total: over €11 million

protiviti

LYING TO THE EUROPEAN COMMISSION

Offender	Facebook
DPA	the European Commission

Facts

- FB purchased WhatsApp in 2014 for $19B.
- When questioned by the EC, Facebook claimed to be unable to automatically link the accounts of both Facebook and WhatsApp users.
- FB claimed in reply to a follow-up query from the EC that automatically matching FB and WA was not possible.
- By August 2016, WhatsApp announced that it would start sharing its data, including users' phone numbers, with Facebook, in order to help target ads.
- The EC was not amused.

NOT VETTING SUB-CONTRACTORS

- "The commission considers that Facebook staff were aware of the user-matching possibility, and that Facebook was aware of the relevance of user matching for the commission's assessment, and of its obligations under the Merger Regulation[.]"

Fine **€110M**

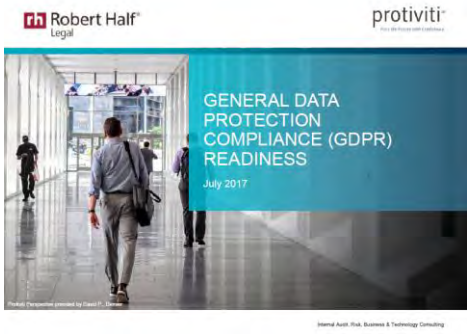
protiviti

ADDITIONAL RESOURCES

AVAILABLE PROTIVITI RESOURCES

Webinars and Roundtables:

- Protiviti and Robert Half Legal hosted a series of GDPR Roundtables to discuss the regulation scope, define the key compliance phases, and identify the right resources and technology to support the compliance program.
- GDPR Readiness Webinar were held in July 2017 and available for instant download

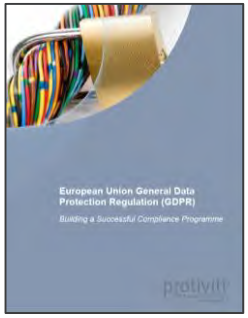


Protiviti Publications:

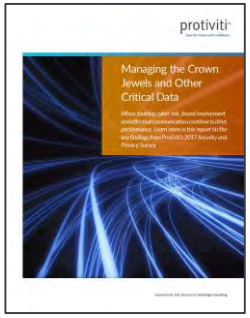
- **Hot Topic Blog Posts**
  - GDPR: Developing Your Compliance Program
  - GDPR: Strict New EU Data Privacy Rules Have Global Reach
  - Internal Audit's Role Will Be Key in the GDPR Journey
- **Thought Leadership**

GDPR Flash Report

GDPR Whitepaper



Protiviti's 2017 Security and Privacy Survey



Board Oversight of Cyber Risk

protiviti

Face the Future with Confidence

protiviti®