



How Organisations can Deliver Accountability under the GDPR



#GDPRinDublin2018

Accountability in GDPR: What It Is and Why It Matters

23 January, Dublin

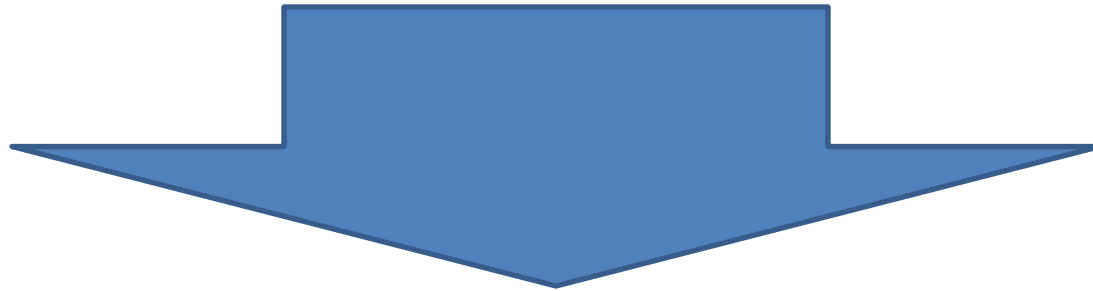
Bojana Bellamy
President

Centre for Information Policy Leadership

Accountability in GDPR = Privacy Programme

Controllers must: (Processors, too, in respect of their obligations)

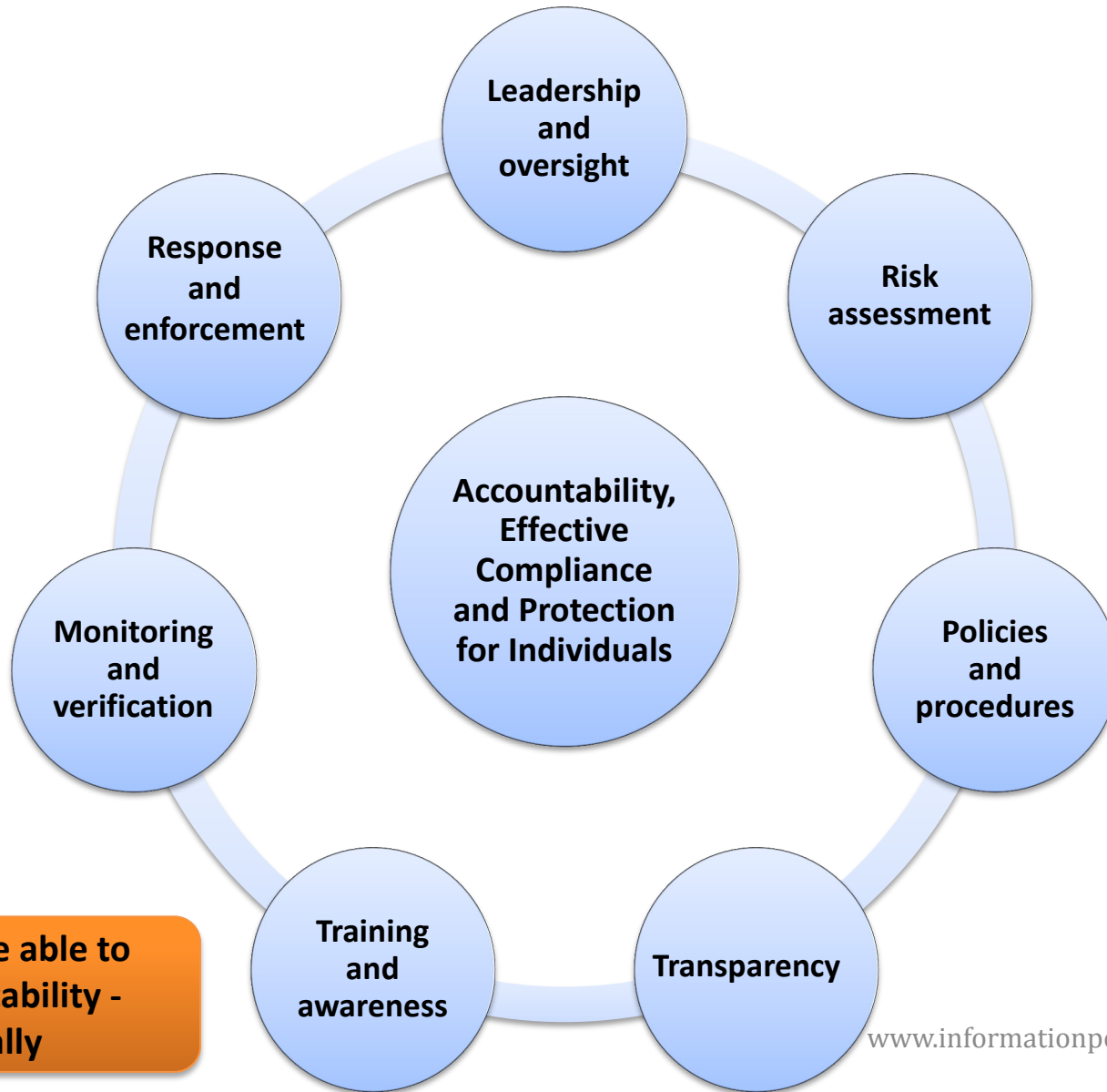
- Be responsible for compliance with GDPR
- Implement appropriate and effective technical and organisational measures to comply with the GDPR
- Demonstrate compliance & effectiveness of the measures



Taking into account:

- The nature, scope, context, and purposes of the data processing
- The risk for individuals - physical, moral, material damages

Privacy Management Programme under GDPR – Universal Elements of Accountability



Organisations must be able to demonstrate accountability - internally and externally

GDPR Accountability – Content of Privacy Management Programmes

- Board oversight
- Senior management endorsement
- Data Privacy Officer/Office oversight and reporting
- Data privacy governance and accountability

Leadership & Oversight



- At program level
- At product, service, and requirement level
- DPIA for high risk processing
- Risk to organisation
- Risk to individuals

Risk Assessment



- Codified internal privacy rules based on DP principles
- Security policies
- Legal basis and fair processing
- Vendor/Processor management
- Individual rights handling
- Other, e.g. Marketing rules, HR rules, M&A due diligence
- Data transfers mechanisms

Policies & Procedures



- Templates and tools for privacy impact assessments
- Privacy by Design process and checklists
- Privacy engineers

Privacy by Design



- Privacy policies and notices to individuals
- Innovative transparency – dashboards, integrated in products/apps, articulate value exchange and benefits, part of customer relationship
- Access to information portals
- Notification of breaches

Transparency



- Mandatory corporate training
- Ad hoc and functional training
- Awareness raising campaigns and communication strategy

Training & Communication



- Internal record of processing
- Documentation and evidence - consent, legitimate interest, notices, PIA, processing agreements, breach response
- Internal verification and self-assessments
- Internal audits
- External verification/audits
- Seals and certifications

Monitoring & Verification



- Individual complaints handling
- Breach reporting, response and rectification procedures
- Managing breach notifications to individuals and regulators
- Internal enforcement of non-compliance
- Engagement/Co-operation with DPAs

Response and Enforcement



**Organisations must be able to demonstrate
- internally and externally**

GDPR Accountability – Self-Enlightened Interest of Organisations

Proactive data management is a business issue; accountability > legal compliance

Enable new business models, digitalisation, globalisation and data-driven innovation

Address increased expectations of individuals for transparency, control and value exchange

Ensure data protection, sustainability and digital trust

Address regulatory change, impact and implementation

Mitigate legal, commercial and reputational risks

GDPR Accountability – Benefits for DPAs and Individuals

DPAs

Reduces enforcement and oversight burden of DPAs

Promotes constructive engagement with accountable organisation

Enables leverage of peer pressure and “herd” mentality

Individuals

Effective protection and reduced risk/harm

Empowered, able to exercise rights and complaints

Trusting and ready to benefit and participate in digital society

GENERAL DATA PROTECTION REGULATION

PERSONAL DATA
GLOBAL IMPACT

ACCOUNTABILITY
DUBLIN
JANUARY 2018

ACCENTURE BACKGROUND



WHO ARE WE?

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

WHAT HAVE WE DONE IN PRIVACY?

Accenture has a **Compliance Framework** and **Global Data Privacy Program** including our **Data Privacy Policy**, **Binding Corporate Rules** and a **Global Data Privacy Team** with currently 35 people (core) + extended DPIS team. Also, Accenture has a strong – ISO certified - **Information Security Program** in place.

FIVE ELEMENTS OF ACCOUNTABILITY DATA PRIVACY PROGRAM

Leadership	<ul style="list-style-type: none">• Global team of resources led by Senior Director, Data Privacy• Part of CORE Ethics and Compliance Legal function• External relations activity (for example on the EU GDPR)• Data Privacy Officer appointed• Formalized, standardized, consistent and trained DPO network in all GUs
Risk Assessment	<ul style="list-style-type: none">• Early identification of privacy trends, developments and legislative changes and assessing their impact on Accenture• Global Risk Assessments and program reviews conducted on a periodic schedule with program enhancements implemented
Standards and Controls	<ul style="list-style-type: none">• Policy 90 (Data Privacy) and our Binding Corporate Rules are our foundation rules for processing Accenture personal data and international transfers• Supplemented by system/function specific data privacy statements and governance standards and processes• Client Data Protection Program, Policy 1431 (Data Management) and client contracts (including EU model clauses) govern Accenture's processing of client personal data and international transfers• Privacy by Design - designing our offerings in a way that takes data privacy compliance into account• Regulatory registrations - handled by local Data Privacy Officers or Geographic Legal Leads• Supplier Management - handled by IS and Procurement• M&A/JV due diligence – includes data privacy• Policy 1413 (Corporate records) – includes rules on retention of Accenture personal data*

FIVE ELEMENTS OF ACCOUNTABILITY DATA PRIVACY PROGRAM

Training and Communication	<ul style="list-style-type: none">• Mandatory information security/data privacy training for new joiners• Data Privacy Community of Practice• International Data Privacy Day activities• Regular program of communication, awareness and training• GU Information Security & Data Privacy Leads accountable for i. enforcing global communications / training ii. identifying local initiatives required and iii. a defined local SME within each GU
Monitoring, Auditing and Response	<ul style="list-style-type: none">• Incident Response & Triage Desk for security incidents involving personal data• Complaints handling and exercise of rights by individuals - handled by local Data Privacy Officers/HR• Audits, Reviews & Monitoring – there have been internal and external ad hoc audits and a regular program of audit and monitoring is under development
The PLUS: Ethics & values	<ul style="list-style-type: none">• Privacy doesn't equal compliance – you need to recognize its ethical aspects and build it onto values: doing the right things right• In addition, the Data Privacy team provides a range of support, advice and input on new offerings, client bids, contracts and engagements and to Corporate Functions (for example on internal data use, Marketing, roll out of new CIO tools, surveys etc.)• Thought leadership, points of view

COMMON GROUND: RE-USING INFORMATION

A subset of information is relevant throughout the lifecycle – consider one repository which you leverage each time.
In particular, but not limited to the following:



LEGITIMACY

- Assessing legitimacy of processing activities (e.g., art. 5, 6) requires sufficient understanding of relevant aspects



PROTECTION BY DESIGN & DEFAULT; DPIA

- Understanding processing, aims & means (art. 25)



INFORMATION & ACCESS

- Informing individuals of processing, providing access and responding to access requests (e.g., art. 13, 14)



CONTRACTS: MINIMUM CONTENT

- Relevant content for contracts (e.g., art. 28 para. 3)



INCIDENT MANAGEMENT

- Have relevant information at hand to assess risks swiftly and notify regulator and/or data subjects (art. 34, 35)

← ACCOUNTABILITY →

EXAMPLE DOCUMENTATION REQUIREMENTS(1): CONTROLLER ROLE

Area	Comments
Name and contact details.	Include the contact details for the data controller (i.e. Accenture or a third party data controller for whom Accenture acts as a data processor), the representative of the data controller and the data protection officer.
The purposes of the processing activity.	<p>List the purposes clearly and precisely.</p> <p>This should be as specific as possible – if Accenture refers to a general purpose description (e.g. “<i>control of the workplace</i>”), such general description should be completed with a more specific purpose such as “<i>control of professional activities at the workplace via cameras, control of emails, internet usage, telephone</i>”.</p>
Description of the categories of individuals.	<p>Accenture must list the categories of individuals of whom the personal data are processed.</p> <p>It is not necessary to list each individual by name – it is sufficient to include categories of individuals. Examples of categories of individuals may be employees, contact persons at customers, or contact persons at suppliers.</p>
Description of the categories of personal data.	<p>Accenture must list the categories of personal data that are being processed.</p> <p>Examples of categories of personal data are identification data, financial data, health data, audio data and videotapes.</p>
The categories of recipients.	<p>Accenture must include the categories of recipients to whom the personal data have been or will be disclosed. This includes both internal recipients (i.e. other Accenture entities) and external recipients (e.g. suppliers that have access to the personal data).</p> <p>Accenture is not obliged to list all recipients individually – it is sufficient to only include categories of recipients. Examples of categories of recipients may be employers, marketing companies, the government, judicial authorities and subsidiaries.</p>

EXAMPLE DOCUMENTATION REQUIREMENTS (2): CONTROLLER ROLE

Area	Comments
Transfers of personal data to a non-EEA country or an international organization.	<p>The register should specify if a transfer to a non-EEA country has taken place.</p> <p>There is no need to mention the safeguards on which such transfer has been based, such as standard data protection clauses or binding corporate rules.</p>
Retention period.	<p>Accenture must include the envisaged retention period for the different categories of personal data.</p> <p>It is not necessary to specify days, months, years, or provide a quantitative assessment. It is possible to refer to certain parameters (such as the time needed to achieve the specific purpose pursued or the expiry of a limitation period).</p>
A general description of the technical and organisational security measures.	<p>Include a concrete and easy to understand description of the measures, which is sufficiently specific for the supervisory authorities to carry out an initial review of the legality of the processing activity.</p> <p>Examples are: pseudonymization measures, encryption measures and a description of the procedures for periodical reviews of the effectiveness of such measures.</p>
Legal basis	<p>Identify specific legal basis (art. 6 and/or specific legislation)</p>

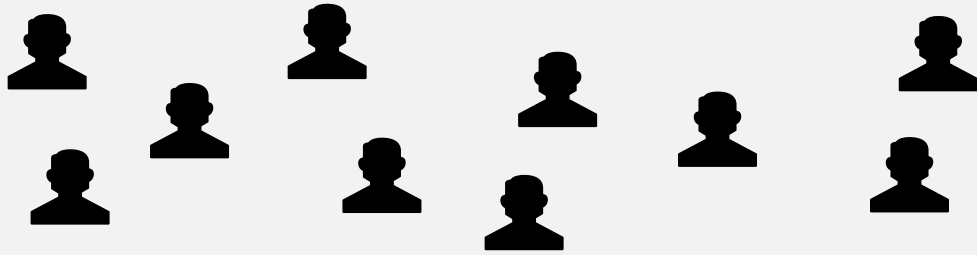
DOCUMENTATION: GUIDANCE ON GRANULARITY CONTROLLER ROLE

Granularity	<p>Requirement to maintain a record of <u>each processing activity</u>.</p> <p>We adopt the following approach with regard to the register which we maintain as a data controller:</p> <ul style="list-style-type: none">• where a processing activity has multiple purposes, we adopt a granularity of one entry for each processing activity with a distinct purpose – if a processing activity has multiple purposes, multiple entries should be used.• where multiple entities (that are each separate data controllers) perform similar processing activities, a separate entry should be used for each such entity. <p>This ensures that if a DPA asks to see a register of all processing activities of a given Accenture entity, Accenture can provide those processing activities that are relevant to such entity.</p>
Example	<p>If the HR departments of our regional companies in France and Germany send (each for its own purpose and at its own initiative) communications to their employees, such processing activity will have multiple purposes – such as payroll management and compliance investigations.</p> <p>In this example, entities should include 4 separate entries: (i) HR communications by regional entity France for payroll administration, (i) HR communications by regional entity Germany for payroll administration, (iii) HR communications by regional entity France for compliance investigations and (iv) HR communications by regional entity Germany for compliance investigations.</p>

WE HAVE DEPLOYED A NETWORK OF DP SME'S ACROSS THE GUS ADDRESSING PAST CHALLENGES

Pre 2018

Data Privacy Team



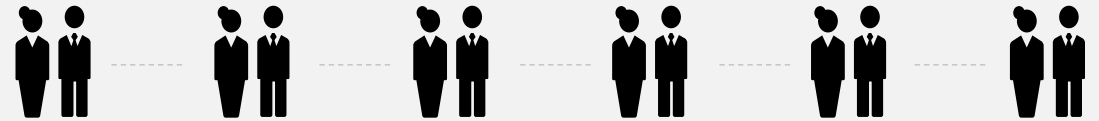
Network Characteristics

- Limited central accountability for regulatory activity
- DPOs deployed to individual countries
- Inconsistent grading and experience of DPOs
- Different deployed to entities for different DPOs
- Varied FTE allocation to country DPO role
- Inconsistent formal line reporting / governance / model

From 2018

Data Privacy Team

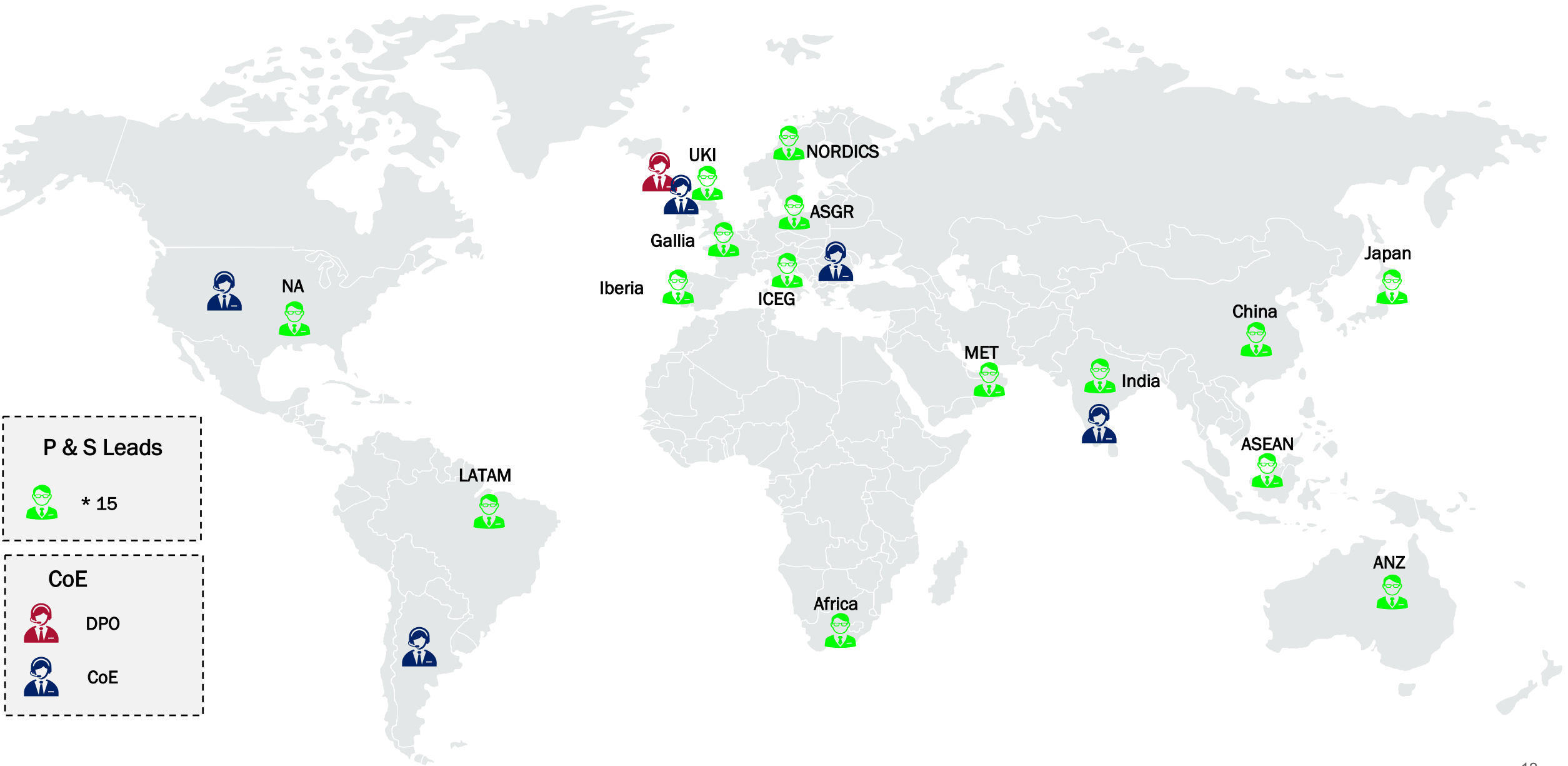
Centre of Excellence




Network Characteristics

- ✓ Single DPO appointed to be accountable for all matters with DP regulators
- ✓ GU level Data Privacy and Information Security Role deployed creating a connected network of peers
- ✓ Standard grading CL6 – Senior Manager
- ✓ Full time role
- ✓ Standard deployment into Geographic Services
- ✓ Data Privacy Sponsor role created for local escalations
- ✓ Defined set of global governance meetings established
- ✓ Extensive FY18 training plan deployed - to continue in FY19
- ✓ Centre of Excellence created – dedicated to support GU Leads


GLOBAL DATA PRIVACY OFFICER NETWORK




P & S Leads

 * 15

CoE

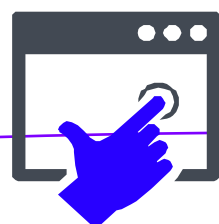
 DPO

 CoE

THE DATA PRIVACY OFFICER NETWORK LEARNING JOURNEY



Jan - Feb I attend weekly virtual calls to learn about various topics



I'm taking GDPR courses in myLearning



At the DP Summit, I meet and network with my colleagues, face to face



I learn how to be a trusted advisor, so I can successfully navigate the organization and talk with senior leaders



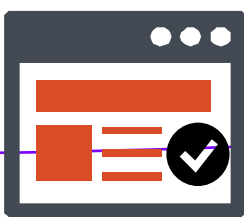
I PARTICIPATE IN CASE STUDY SCENARIOS WITH COLLEAGUES TO BETTER UNDERSTAND HOW TO APPLY THE NEW REGULATIONS



I learn about the DPO Organization and learn when and how to connect with relevant colleagues



After the DP Summit, I attend monthly calls to share lessons learned and ask questions



I complete these Certifications:
1) GDPR Ready Training (IAPP) and
2) ISO 27001 Lead Auditor Training



I understand the regulations, can apply them appropriately, can discuss them with colleagues and continue to share lessons learned with the network



hp

DATA MAPPING

Assessments

Status: All Assessments | All Templates: Asset | Clear Filters

ID	Name	Type	Status	Organization
53	Supplier Referenc...	Asset	Under Revi...	HP
52	PLCM-PMG (HPI)	Asset	Under Revi...	HP
49	eCommerce Servi...	Asset	Under Revi...	L2: IT
44	Payment Gateway...	Asset	Under Revi...	L2: IT
43	Workday HPI	Asset	Under Revi...	L2: IT
42	SDM	Asset	Under Revi...	L2: CTO Engineeri...
41	Saba/Grow @hp (...)	Asset	Under Revi...	L2: IT
40	✓			

Secondary Menu:

- ✓ Welcome
- Dashboard
- Assessments
- INVENTORY**
- Assets
- Processing Activities
- REPORTING**
- Asset Map
- Cross-Border
- Scan Results

Understand assets and associate basic data governance (storage etc.)

★ Welcome

- Section 1 ▶ Asset Information
- Section 2 ▶ Security
- Section 3 ▶ Disposal
- Section 4 ▶ Processing Activities
- Section 5 ▶ Feedback

Associate assets to processing activities....

HP | Hello M

DATA MAPPING

✓ Welcome

Dashboard

Assessments

INVENTORY

Assets

Processing Activities

REPORTING

Asset Map

Cross-Border

Scan Results

SETUP

Asset Template

Processing Template

Data Elements

(Pilot) CID Person Customer ID

UNDER REVIEW

Processing Activities

✓ — — — — ✓

What (Personal Data) Processing Activities does (Pilot) CID Person Customer ID Support?

Select one or more from list or add / propose new activities by typing in the box below. As more questionnaires are completed and approved the list will grow. If adding to the list, you can add more than one. For any new processing activities you add you will be asked to identify a contact name.

Not Sure

General and Marketing Consent | L2: IT

Person Identification | L2: IT

Survey of processing activities to capture other data protection elements (legal basis, transfer, controller vs. processor)

How Can Controllers & Processors Build Accountability under the GDPR

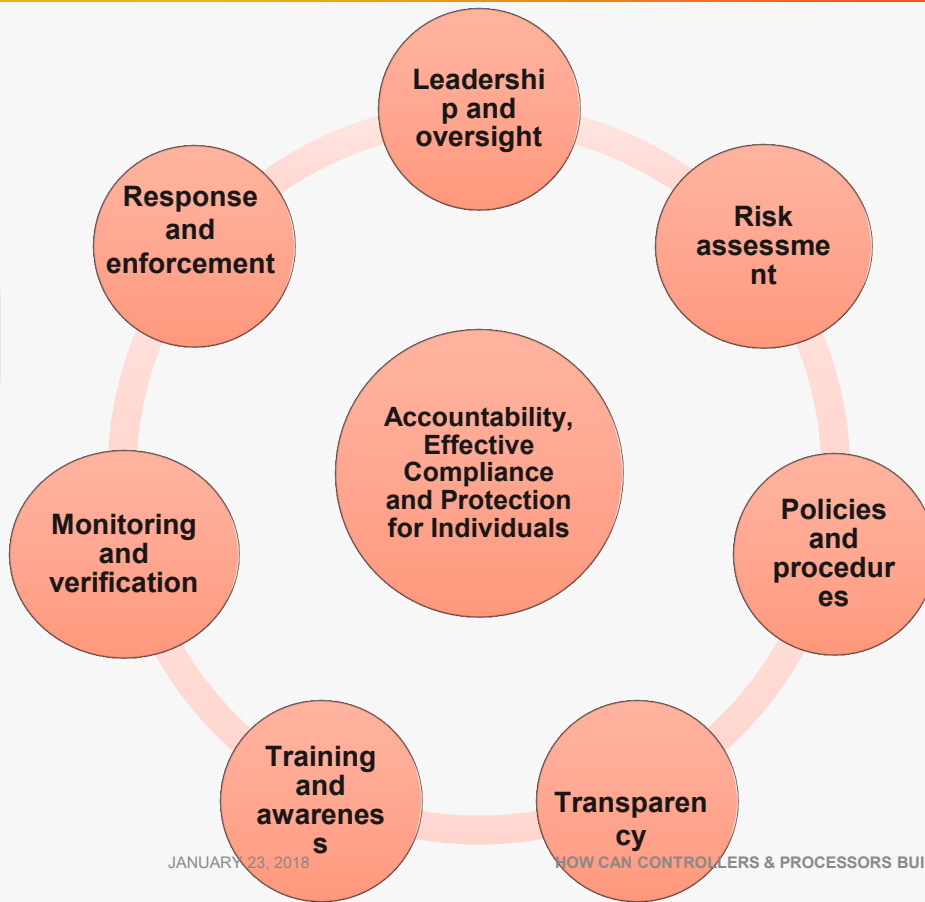
Demonstration & Documentation

January 23, 2018



Privacy Management Programme under GDPR – Universal Elements of Accountability

Organisations must be able to demonstrate accountability - internally and externally



GDPR Accountability – Content of Privacy Management Programmes

**Demonstrate
Accountability to
internal & external
stakeholders**

- Board Commitment
- CEO and Executive Committee
- Dedicated Privacy Officer & Office
- Information Governance

Leadership & Oversight



- Data Risk Framework
- Privacy By Design Process
- Legitimate Interest documentation
- Data Protection Impact Assessment

Risk Assessment



- Security policies
- Privacy policies
- Vendor management
- M&A due diligence
- Data transfers - BCRs

Policies & Procedures



- Templates/tools for privacy impact assessments
- Privacy by Design tools
- Engagement with business, technology team

Privacy by Design



- Privacy policies and notices to individuals
- Innovative transparency – within product design
- Breach Notification

Transparency



- Mandatory corporate training
- Functional Training
- Awareness campaigns

Training & Communication



- Data Inventory
- Data Maps of Processing – including legal bases
- Consent Management
- Reviews/Audits

Monitoring & Verification



- Individual Rights Management
- Breach reporting
- Internal enforcement of non-compliance
- Engagement/ Co-operation with DPAs

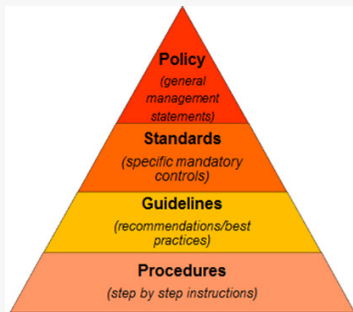
Response and Enforcement



Mastercard's Privacy & Data Protection Program

Mastercard's program has been built to ensure compliance, enable innovation and be responsive to the evolving regulatory landscape

Compliance



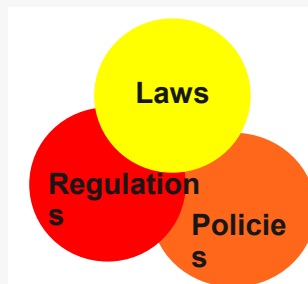
- Legal Inventories
- Policies, Standards, Procedures
- Regulatory Requirements
- Data Transfer solutions
- Breach notification
- Audits/Reviews

Privacy By Design



- Ensures privacy/data protection requirements are addressed as part of product design
- Work as a key business advisor
- Ensure accurate system and process implementation

Regulatory



- Monitor new and pending laws and regulations
- Proactive incorporation into product design thinking
- Regulatory outreach to explain business implications of new law

Training & Development



- Provide training
- Understand privacy requirements in all business areas
- Create key business partnerships and drive controls

APPROACH



LEGAL ANALYSIS

- Understand legal requirements for all data driven activities
- Identify impacts to various business and operational activities – scheduled training sessions



INITIAL ASSESSMENT

- Information Governance and Data Privacy team conducted 60+ training sessions globally over a six-week period
- Information Governance conducted detailed workshops to review the GDPR requirements and determine business & technical impacts
- O&T and Business teams produced high level estimates by business unit



DESIGN WORKSHOPS

- For each in scope data activity identify the changes required – Business Process, Technical and Contractual – and associated costs
- Workshops to be attended by a cross-functional group of subject matter experts, business, technical & legal representatives



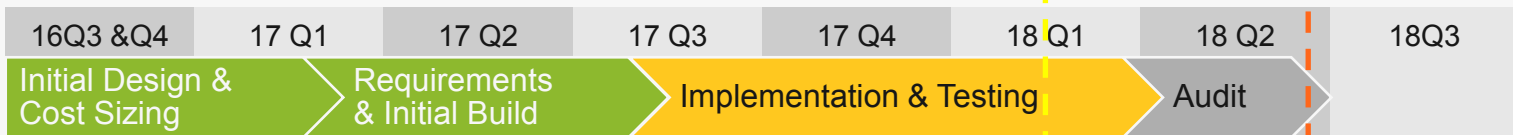
IMPLEMENTATION PLAN

- Confirm scope, impact & refine budget
- Develop enterprise solutions for common problems, benchmark solutions
- Minimize cost and improve data utility for future use
- Create detailed implementation roadmap and timeline for each business and technical team

GDPR Project Timeline

Today

Deadline
May 2018



TECHNOLOGY

Enterprise Solutions

- Data Access
- Data Inventory
- Consent

- ✓ Compliance requirements identified
- ✓ Design sessions conducted with business & technology teams

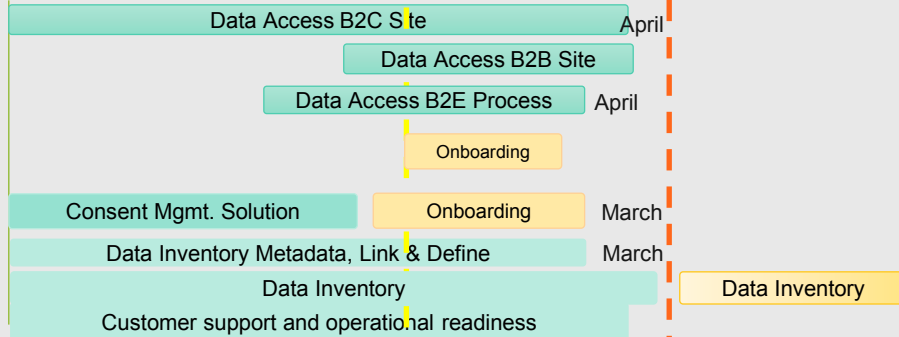
- ✓ Enterprise technology teams established & design solutions finalized
- ✓ Business unit technology solutions identified

Business Units System Changes

- Integration with Enterprise Solutions
- Websites & Apps updated

- ✓ Initial solutions identified

- ✓ Technology build/changes in progress

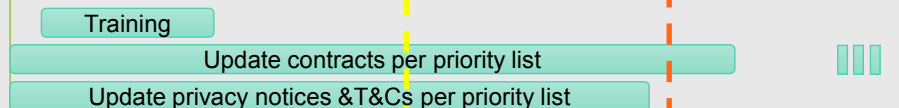


LEGAL

- Rules
- Contracts
- Data transfer mechanisms
- Engagement with issuers

- ✓ Rules changes identified
- ✓ Contract changes identified
- ✓ Privacy Notices/T&Cs

- ✓ Contract amendments drafted & negotiations commenced
- ✓ Meetings with Issuers to discuss cooperation procedures



TRAINING

- General Training
- Role Specific Training
- One Pagers for Data Collection

- ✓ Update Privacy & Data Protection Training
- ✓ Ensure data protection requirements are

- ✓ Create role specific training materials
- ✓ Create simple business guides/one pagers



mastercard

met

JANUARY 23, 2018

HOW CAN CONTROLLERS & PROCESSORS BUILD ACCOUNTABILITY UNDER THE GDPR

MasterCard Activity: Franchise Integrity – Account Data Compromise

Mastercard Role: [Controller](#) | Mastercard Category: Core & B2B

Legal Basis: [Performance of an Agreement](#)

MasterCard Activity Description: To mitigate fraud occurring on MasterCard-branded payment cards and card acceptance locations and to manage risk within the MasterCard system for the benefit of Issuers and Acquirers and to manage MasterCard brand risk, MasterCard monitors transactions and merchant activities for potential fraud and prevention of fraudulent transactions. After fraud occurs, Issuers and Acquirers report activity to MasterCard for additional analyses, monitoring, and future prevention. In addition, MasterCard analyzes MasterCard-branded payment card spend data to identify patterns indicative of fraud that can assist an issuer in assessing the risk of fraud associated with specific card accounts as a result of those accounts having been exposed to an account data compromise event.

MC Application / System / Process	Data Elements Collected / Used / Data Subjects (PII and Sensitive Data)	Data Source / Geography / Transfer	MC Activity	Approach to Notice & Consent (where applicable)	Third Parties Receiving Data	Data Retention	Security / Integrity
<ul style="list-style-type: none"> ADC Operational Reimbursement/Fraud Recovery Data Warehouse Fraud Data Warehouse Fraud Reporter System to Avoid Fraud Effectively (SAFE) Manage My Fraud & Risk system (BPMS) Access Database (ADC Calculations) 	<ul style="list-style-type: none"> Payment Card Account Number (PAN) Card Validation Code (CVC) Merchant ID Issuer/Acquirer Business Contact Details: Name, Address, Phone, Email Merchant Business Contact Details: Name, Address, Phone, Email (occasionally) 	<p>Data Source:</p> <ul style="list-style-type: none"> Issuer Acquirer <p>Collected In:</p> <ul style="list-style-type: none"> USA EU <p>Transferred To:</p> <ul style="list-style-type: none"> USA <p>Purpose of Transfer: Fraud and Risk Mitigation</p>	<p>Activity 1</p> <ul style="list-style-type: none"> Issuers report to MC suspected points of compromise Acquirers report to MC Merchants processor suspected compromises Monitoring of public sources (media, Krebs on Security, FICO Forum blogs) Notify acquirers that they need to perform forensic investigation Once compromise and scope and timeframe of breach is confirmed we send Alerts with generic merchant/processor info, timeframe and associated PANs (acq provided or internal) ADC appeal handling (ADC User Guide & Security Rules & Procedures) <p>Legal Basis:</p> <ul style="list-style-type: none"> Performance of an Agreement 	<p>Notice:</p> <p>Mastercard:</p> <ul style="list-style-type: none"> Reminds Issuer and Acquirer of potential Notice obligation via Standards Provides Notice via Global Privacy Policy Provides Notice via MC Application/System Privacy Policy <p>Issuer/Acquirer:</p> <ul style="list-style-type: none"> As Appropriate, provides Notice to cardholder, merchants, and employees Best Practices Manual ADC User Guide <p>Consent: (if applicable)</p>	<p>Vendor Fox IT (POC only)</p> <p>Roles of Parties</p> <ul style="list-style-type: none"> Analyze merchants for potential software/system infiltration 	<p>See “<i>MasterCard Worldwide Data Retention Policy</i>”</p>	<p>See “<i>MasterCard Worldwide: Analysis of Information Security Safeguards</i>”</p>



Language Matters

Design Jam Team | CIPL | Feb 22nd



Elaine Montgomery

Design Manager, Facebook

Chris Downs

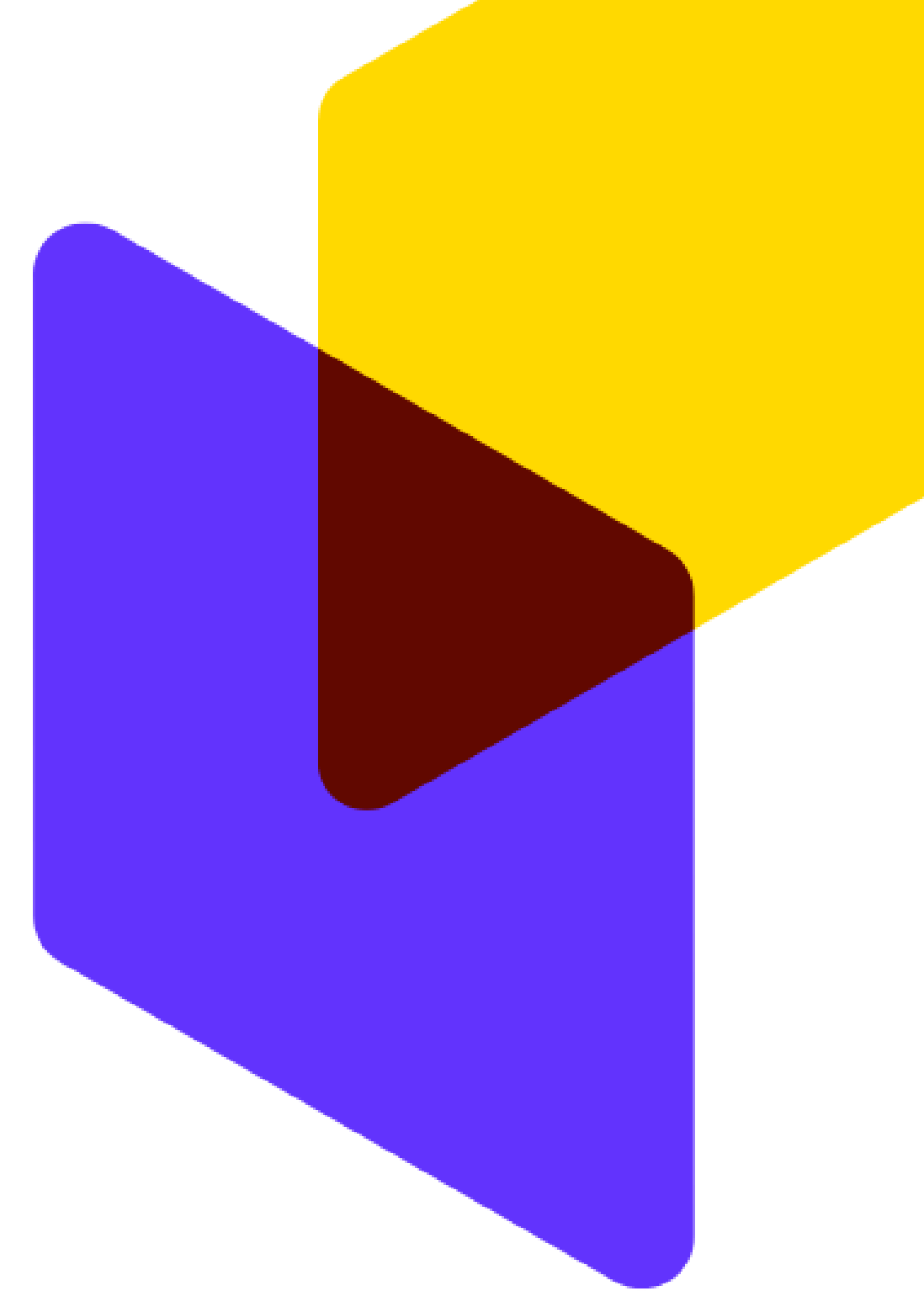
Managing Director, Normally



Design Exercise – Language Matters

We'll spend the next 30 mins doing a design exercise.

We use this exercise (and others) in 1-day Design Jams where we bring together industry, design, policy, legal and regulators to co-create new user experiences for trust, transparency and control.



What constitutes clear and transparent language?

We use the 'Language Matters' exercise to highlight the interplay between legal precision and simple, straightforward, human language.



Simple

1000 songs in your pocket.

Jargon

Today we're introducing a new portable music player that weighs a mere 6.5 ounces, is about the size of a sardine can, and boasts voluminous capacity, long battery life, and lightening fast transfer speeds.

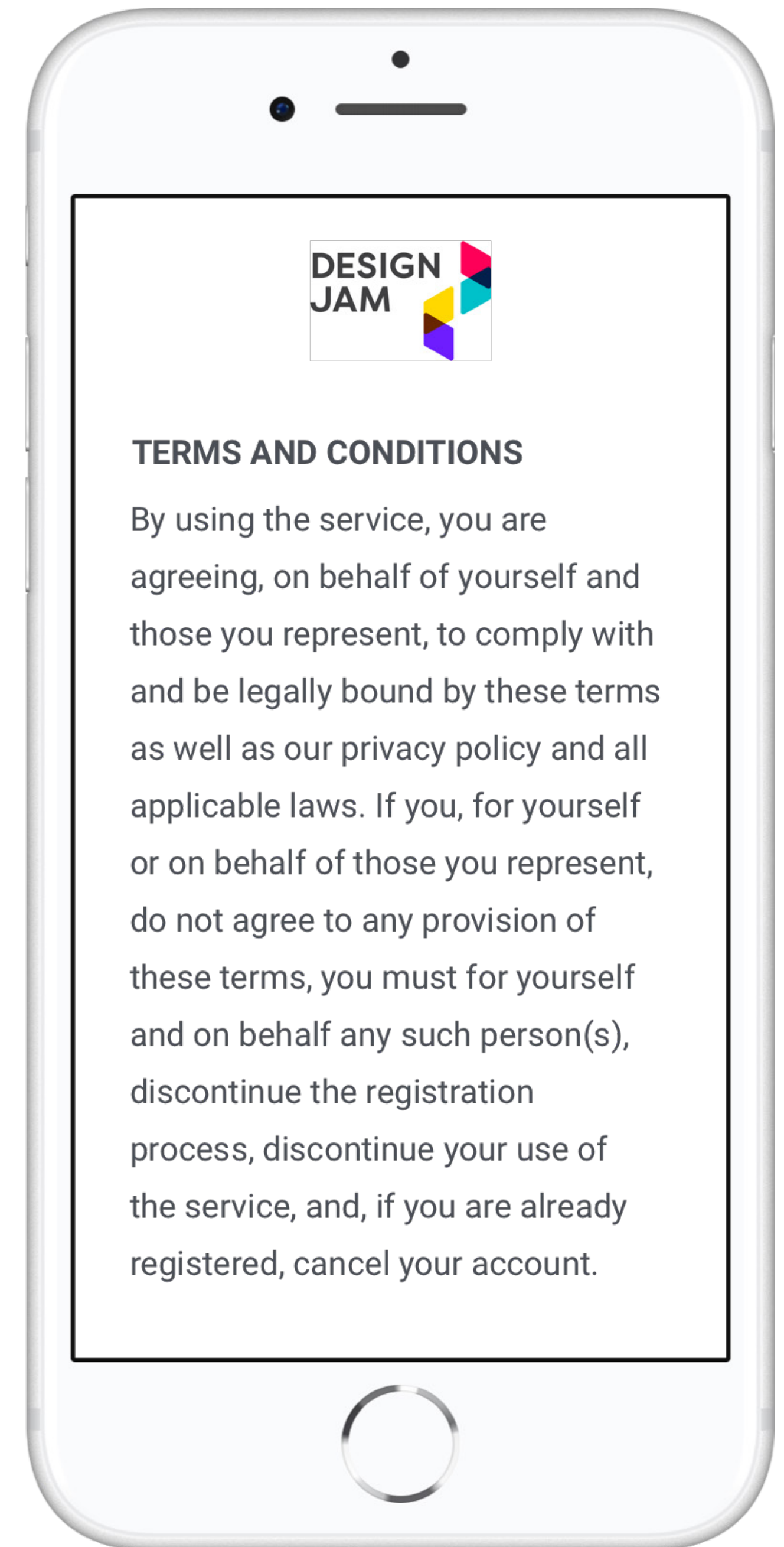
Is it human?

When writing, making it simple, straightforward and human is crucial for transparency & understanding.

Redaction & Re-writing

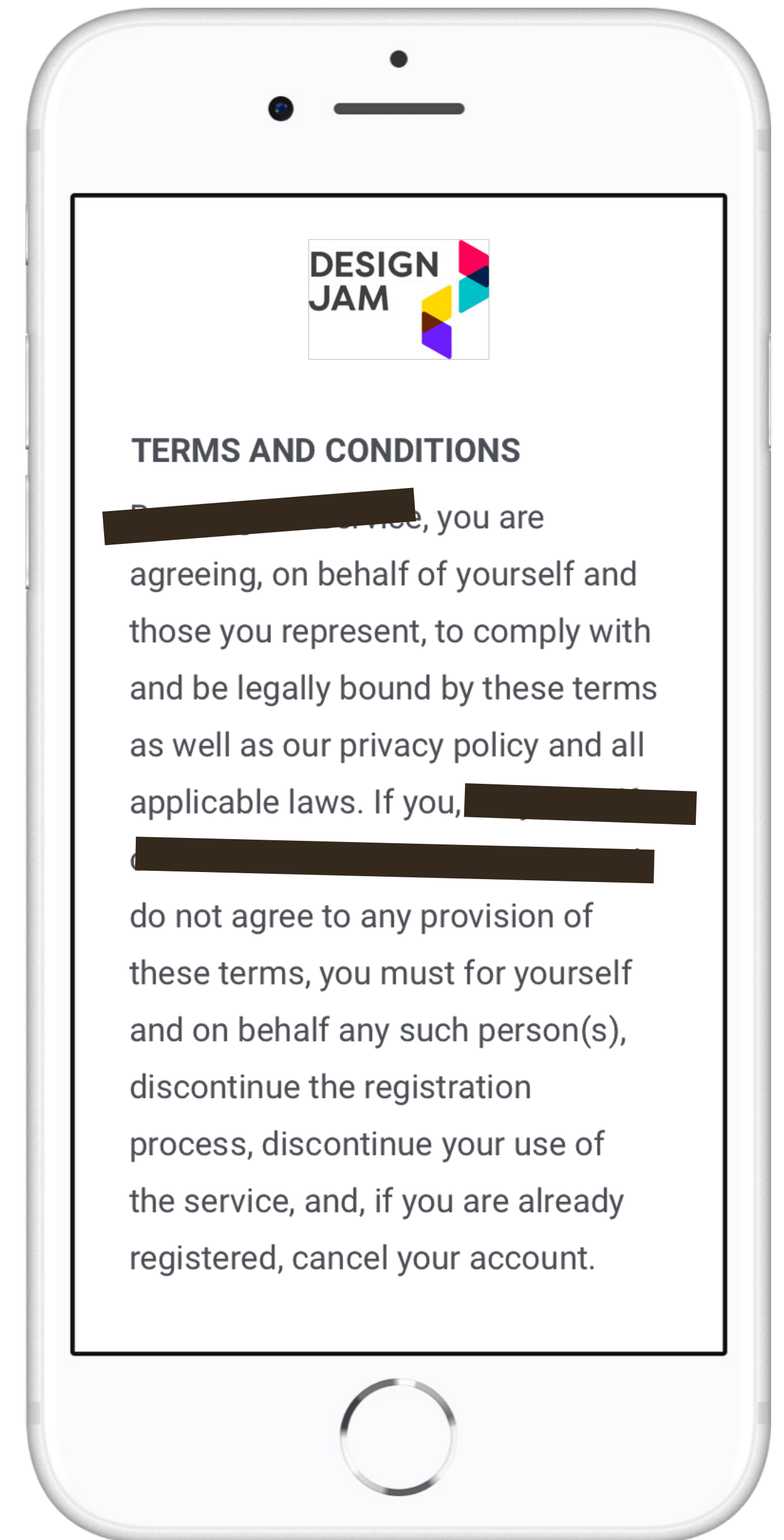
In this exercise we'll be looking at a fictional **Terms of Service** for the Design Jam website. We're going to look at how transparent it is, and how we understand it.

You decide which words are most effective for transparency and understanding.



Redact & Re-write

In teams of 3, discuss first then start removing, adding or re-writing the Terms of Service.



What now?

Look under your chairs
for a **clipboard of
material & instructions**



Divide into **groups of
three** with the people
sitting next to you



You'll have **15 mins** for
this exercise - Let's start!

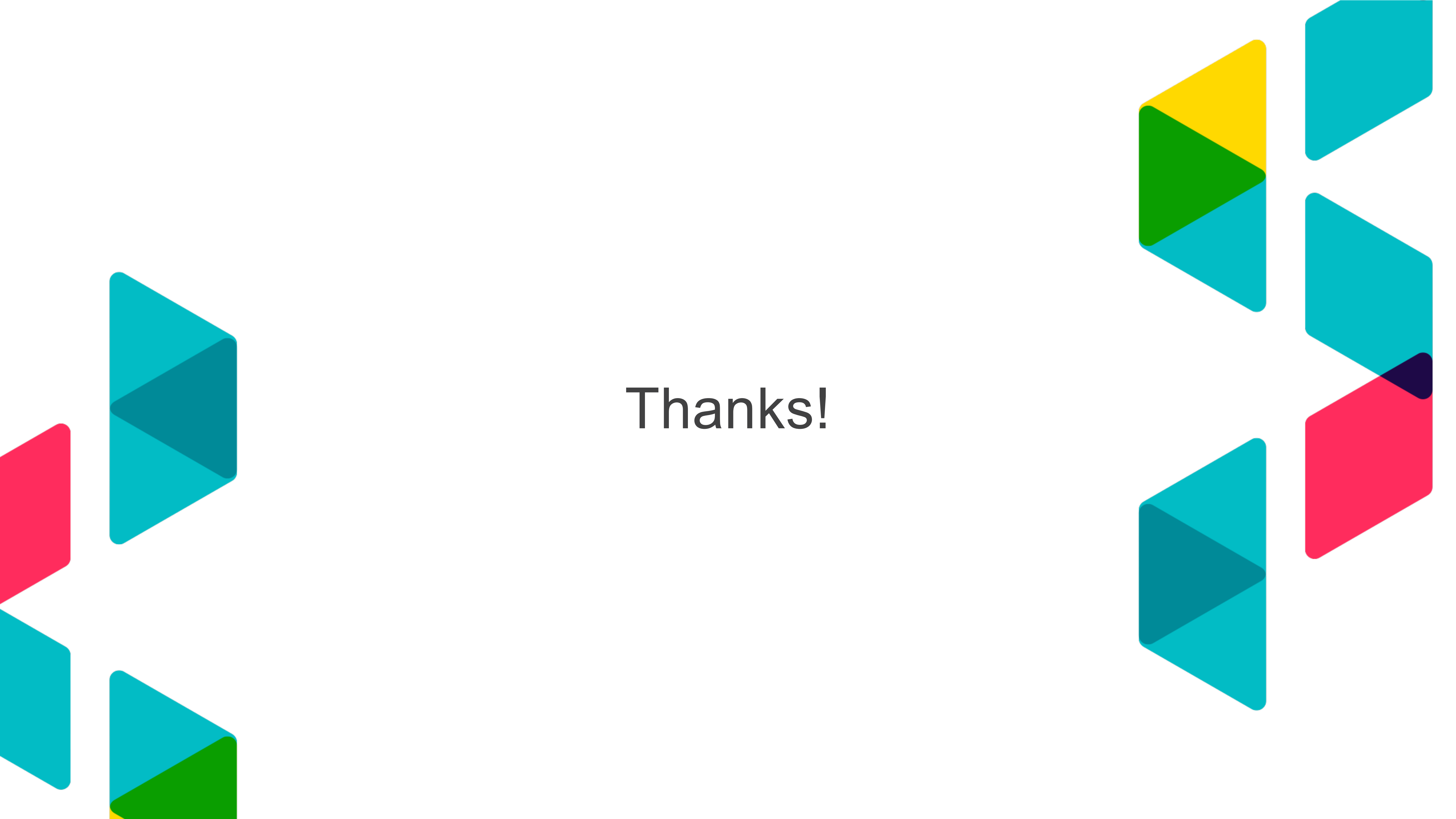


What did we learn?

- Make trade-offs between legal precision & clarity
- Be simple, straightforward and human
- Tone of voice matters
- Not dumbing it down, it's opening it up



Thanks!





Data Protection Impact Assessments

Simon Bristow

Head of Data Privacy, Novartis UK & Ireland

23 January 2018

Data Protection Impact Assessments

Context

- Accountability – technical and organisational measures to ensure and demonstrate compliance
- Measures must take into account data processing activities and risks

Data Protection Impact Assessment (DPIA)

- Structured process to assess data processing risk and demonstrate compliance
- Required for data processing likely to result in ‘high risk’ to rights and freedoms of individuals
- Performed before data processing occurs

Data Protection Impact Assessments

Not just a compliance requirement

- DPIAs offer a range of benefits:
 - Identify and treat risks
 - Demonstrate compliance
 - Avoid last-minute project changes and delays
 - Raise awareness within the business
 - Facilitate compliance with other GDPR requirements
- Highly recommended as good practice, even when not required under GDPR

Approach for DPIAs

- GDPR does not specify a process, but in practice DPIAs follow common key steps

Key steps

Initial assessment

- Determine if processing likely to result in a 'high risk' to individuals
- If not, determine value in performing DPIA as good practice
- Document rationale for performing DPIA or not

Explore data processing activities

- Explore and document data planned data processing
- Consider full lifecycle of data (e.g. collection, storage, transfer, deletion)
- Review data fields and data flows – the devil is in the details
- Involve key individuals, e.g. IT lead, project manager, vendor

Key steps

Assess necessity, proportionality, and risks

- Assess necessity and proportionality of processing
- Assess risks to individuals (likelihood and severity)

Treat risks and consult

- Define measures to treat risks and demonstrate compliance
- Agree ownership of risks and measures
- Consult as required and appropriate (e.g. Data Protection Officer, Commissioner, individuals)

Manage risks

- Continuously monitor risks and measures
- Update DPIA if processing changes

Novartis' approach

Current state

- Assessments performed for new systems and business processes, according to data classification
- In-house tool for assessments based on Swiss law requirements

Future state

- New tool (OneTrust) and updated, globally standardised procedure
- Use tool and process to build record of data processing activities
- Simplify process and define roles and responsibilities

Risk and Control Self-Assessment (RCSA) framework

- Global framework to identify and control risks of global business processes and their local implementation
- Build accountability and ownership of business functions

GENERAL DATA PROTECTION REGULATION

MANAGE RISK
WITH **DPIA**
DUBLIN
JANUARY 2018

ASSESSING THE RISK WITH A DPIA PROCESS

BACKGROUND ON ACCENTURE

WHO ARE WE?

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 435,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

WHAT HAVE WE DONE IN PRIVACY?

- Accenture has a **Compliance Framework** including a **Global Data Privacy Program**, our **Data Privacy Policy**,
- **Binding Corporate Rules** and a **Global Data Privacy Team** with about 35 people. Also, Accenture has a strong **Information Security Program** in place.
- Our Global Data Privacy team has a **privacy impact assessment** process and a specific global review approach combined with other legal reviews for global rollouts.
- Accenture started to work on our GDPR project three years ago assessing impact and gaps and then kicked off deployment team around 12 months ago.
- Iterative approach including “stage gate approach”.

WHAT IS A DPIA?

The aim of the DPIA is a formal **assess the risk of a processing activity** and to assess how such risk can be decreased through the implementation of measures and safeguards

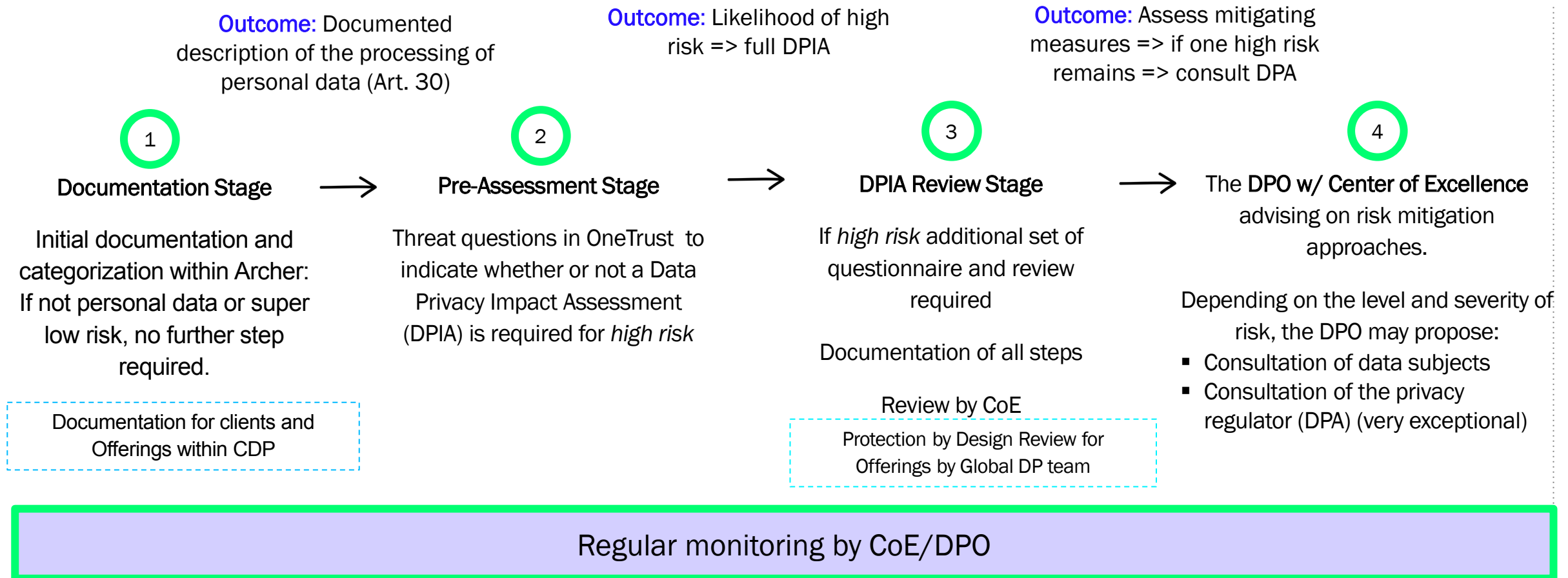
Is the processing activity involving personal data ?

Is there a legal bases and is there an impact to individuals?

Is the processing activity **likely to result in a high risk to the rights and freedoms** of such individuals?

Has Accenture implemented **measures and safeguards** that minimize the high risk to the rights and freedoms to the individuals?

DPIA APPROACH PROCESS



HOW TO DESIGN A DPIA PROCESS?

CHALLENGES AND LEARNINGS

CHALLENGES	LEARNINGS
Identify the gaps and defining the process	Instead of tweaking existing processes add a new DPIA process!
Finding the right data for the DPIA process	Don't invest too much time of trying to find the right data - rather start from scratch
Accountability of the process	Accountability to conduct a DPIA is with the business owner of the process – should not be with DP or DPO – Identify roles per asset
Getting the “right” tool	There is no “wrong” tool- don't loose time for tool evaluation - focus on modifying for your needs
How to define the risks?	Go with an initial approach but plan time to re-evaluate

WHEN IS A DPIA REQUIRED?

PRE-ASSESSMENT – IDENTIFY THE HIGH RISK

If either one **MUST DO** criteria or two or more **MAY DO** criteria applies, a **DPIA** has to be conducted

MUST DO

Scenarios always deemed to likely result into a high risk (Art. 35.3 GDPR):

1. Decision taken based on
 - **Systematic** and **extensive** evaluation of personal aspects and
 - Based on **automated processing** (incl. profiling) and
 - Has a **legal/significant affect** on individual
2. Processing sensitive data or data relating to criminal conviction and offences **at large scale**
3. Systematic monitoring of publicly accessible area **at large scale**

MAY DO

More than two risk triggers as of A29 WP guidance:

1. Evaluation or **scoring** of individuals
2. Observing, **monitoring** or controlling individuals
3. Processing **sensitive data** or data of a highly personal nature
4. Processing data on a **large scale**
 - Number of individuals
 - Volumes and different types of data
 - Duration of processing
 - Geographical extent of the processing
5. Matching or combining datasets from **different sources**
6. Processing data related to **vulnerable individuals** (incl. employees)
7. Processing data in an **innovative manner** or using **new technology**
8. Processing activity could **prevent exercising a right**

DPIA QUESTIONS APPROACH BASED ON EXISTING DOCUMENTATION

15 Pre- Questions divided into 3 sections:

1. Identify of the data controller
2. Description of processing activity
3. Threshold Questions
 - a. Similar processing activity in place?
 - b. Mandatory scenarios
 - Automated decision making
 - Sensitive data at large scale
 - Systematic monitoring at large scale
 - c. Risk factors whether a DPIA is mandatory (at least two to apply)

41 DPIA Questions divided into 12 sections:

1. Purpose
2. Individuals the data relates
3. Types of personal data
4. Location and systems
5. Retention period
6. Legal basis
7. Necessity and proportionality
8. Transfer of data and recipients
9. Technical and organizational Measures
10. Rights of the individuals
11. Risk identification towards rights
12. Consultation of stakeholders

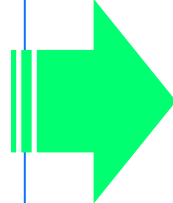


EXAMPLE OF DPIA QUESTION:

LEGAL BASIS/LEGITIMATE INTEREST

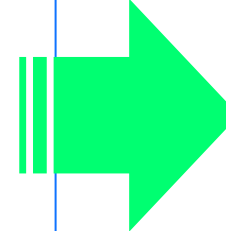
IDENTIFY LEGAL BASES :

1. Processing necessary for the performance of a contract ?
2. Processing necessary for Accenture's compliance with legal obligations?
3. Processing is necessary based on Accenture's legitimate interest ?
4. Processing is based on consent?



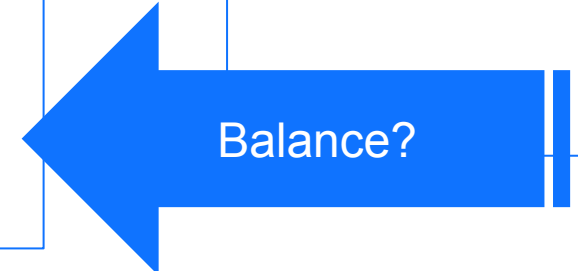
DEFINE LEGITIMATE INTEREST:

- ensuring and verifying that Accenture complies with laws and policies.
- protecting Accenture's reputation.
- managing disputes.
- managing potential corporate transactions.
- ensuring proper communication.
- ensuring handling of emergency situations within Accenture.
- combatting bribery and fraud.
- ensuring security.
- managing its workforce (including by evaluating performance).
- performing projects for clients.
- Other (free text field)



IMPACT TO INDIVIDUAL:

- Describe necessity and proportionality
- Describe the technical and organizational measures
- Transfer to data
- Rights of the individual
- Risk to the individual
- Stakeholder involvement



WHAT ELSE?

- Get expert input
- Document your approach
- Training and Communication is important!
- Consider who will review and sign off?
- Regular monitoring and reporting of DPIA's and pre-assessment
- Review within a certain period of time and adjust (example: conduct a risk assessment)
- Allow iterations – nothing will be perfect in the beginning

APPENDIX

EXAMPLE OF DPIA QUESTIONS:

LEGAL BASIS

<p>This question should be repeated for each purpose selected in question 1.</p> <p>What is the legal basis for the processing of (non-sensitive) personal data?</p>	<p>Drop down menu with the following options:</p> <ul style="list-style-type: none"> the processing is necessary for the performance of a contract between Accenture and the individual. the processing is necessary for Accenture's compliance with a legal obligation. the processing is necessary for the purposes of Accenture's legitimate interests. the processing is justified based on the consent of the individual. 	<p>Describe for each purpose the legal basis on which Accenture justifies the processing of (non-sensitive) personal data.</p> <p>There are 4 common legal bases on which Accenture can rely for the processing of (non-sensitive) personal data. A brief explanation of when you should select each legal basis is set out below:</p> <ul style="list-style-type: none"> the processing is necessary for the performance of a contract between Accenture and the individual. You should select this legal basis where Accenture needs to process the personal data to perform its obligations under a contract with an employee, supplier or customer. For instance: <ul style="list-style-type: none"> Accenture may use the bank account details of an employee to pay such employee the monthly wage agreed in his/her employment contract. for purposes of managing a customer project, Accenture may use the contact details of the customer employee that is listed in the customer contract as the project manager. the processing is necessary for Accenture's compliance with a legal obligation. You should select this legal basis where Accenture needs to process the personal data to fulfil the requirements of under social security laws or other legal obligations. For instance, Accenture may disclose personal data of an employee to a social security institution where it is required to do so under social security laws. the processing is necessary for the purposes of Accenture's legitimate interests. You should select this legal basis where Accenture has a legitimate interest to process the personal data, unless such legitimate interest is overridden by the interests or rights and freedoms of the individuals. For instance, in the context of monitoring of personnel, Accenture has a legitimate interest to review whether its employees complied with the relevant policies (and, if the monitoring is limited to professional documents, the interests or rights and freedoms of the employee are unlikely to be more important than Accenture's legitimate interest). the processing is justified based on the consent of the individual. You should select this legal basis only very exceptionally. Accenture's policy on using consent as a legal basis is as follows: <ul style="list-style-type: none"> you may use consent as the legal basis if you are taking automated decisions based on the profiling of individuals (see numbers 6 and 7). Note that, even with consent, you still have to put in place certain safeguards, such as the right to obtain human intervention. individuals you should not use consent as the legal basis for any other processing of (non-sensitive) personal data. Therefore, to the extent that the other legal bases do not apply, Accenture recommends not undertaking the processing. If you believe that exceptional circumstances justify the use of consent as a legal basis, contact dataprivacy@accenture.com. <p>Note that for consent to be valid, it must be freely given, specific and informed. The individual can also at any time revoke its consent.</p>
--	--	--

EXAMPLE OF DPIA QUESTIONS:

LEGAL BASIS/LEGITIMATE INTEREST

<p>Only display if the answer in question 9 is “the processing is necessary for the purposes of Accenture's legitimate interests”</p> <p>Describe Accenture's legitimate interests.</p>	<p>Drop down menu with the following options:</p> <ul style="list-style-type: none"> ensuring and verifying that Accenture complies with laws and policies. protecting Accenture's reputation. managing disputes. managing potential corporate transactions. ensuring proper communication. ensuring handling of emergency situations within Accenture. combatting bribery and fraud. ensuring security. managing its workforce (including by evaluating performance). performing projects for clients. other. <p>If “other” is selected, free text field.</p>	<p>Describe precisely what legitimate interests Accenture is pursuing.</p> <p>For instance:</p> <ul style="list-style-type: none"> if Accenture reviews its employees' compliance with internal Accenture policies, Accenture's legitimate interest could be described as follows: “monitoring employees so as to verify compliance with the relevant policies”. if Accenture includes contact data of an employee in an organization chart, Accenture's legitimate interest could be described as follows: “creating and maintaining an organization chart with contact data of the relevant employees, so as to facilitate internal communications”. <p>if Accenture retains a database with contact data of its main contact persons with suppliers, Accenture's legitimate interest could be described as follows: “creating and maintaining a database with contact data of the relevant contact persons with suppliers of Accenture, to facilitate communications between Accenture and such suppliers”.</p> <p>List the legal basis on which Accenture can rely for the processing of sensitive personal data. The legal bases for processing sensitive personal data are more limited than those for non-sensitive personal data.</p>
<p>Only display if the answer to question 4 is “yes”.</p> <p>What is the legal basis for the processing of sensitive personal data?</p>	<p>Drop down menu with the following options:</p> <ul style="list-style-type: none"> (for sensitive data other than data relating to criminal convictions and offences) the processing is necessary for Accenture's compliance with a legal obligation under employment or social security laws. (for sensitive data other than data relating to criminal convictions and offences) the processing is justified based on the consent of the individual. (for sensitive data other than data relating to criminal convictions and offences) the processing is necessary to protect the vital interests of the individual. (only for data relating to criminal convictions and offences) the processing is authorised by European law or by the law of the relevant EU country. 	<p>For sensitive personal data (other than data relating to criminal convictions and offences), there are 3 legal bases on which Accenture can rely for the processing of sensitive personal data. A brief explanation of when you should select each legal basis is set out below:</p> <ul style="list-style-type: none"> the processing is <u>necessary for Accenture's compliance with a legal obligation under employment or social security laws</u>. You should select this legal basis where, in an employment context, Accenture must process sensitive personal data to comply with its obligations under employment or social security laws. the processing is justified based on the <u>consent of the individual</u>. You should be careful in selecting this legal basis. Accenture's preference is to use other legal bases than consent for the processing of sensitive personal data. However, to the extent that processing sensitive personal data would be required for Accenture's legitimate business needs, and this processing cannot be justified on any other legal basis, you may select consent as the legal basis for the transfer. <p>Note that for consent to be valid, it must be explicit, freely given, specific and informed. The individual can also at any time revoke its consent.</p> <ul style="list-style-type: none"> the processing is necessary to <u>protect the vital interests of the individual</u>. You should select this basis only where you could not protect a vital interest of an individual without using the sensitive data. This is for instance the case where you use health information to provide first aid services to an employee. <p>For sensitive personal data relating to criminal convictions and offences, the legal bases are even more limited. Such data may only be processed where authorised by European law or by the law of the relevant EU country. If there is no law that authorises the processing of such data, Accenture may not undertake such processing.</p>

Overview - Privacy by design



Policy & Guidance

Training



Tools

Impact Assessment
Documentation



Part A: Privacy @ Google



Privacy Training

Content is tailored to job ladders — product designers and engineers get custom content

Our training is optimized to have the biggest possible impact across the company, ensuring that best practices are taught and reinforced year after year.

Engineers and product managers get special, in-depth training during on-boarding

More than half of our employees are enrolled in this special, in-depth training within three months of hire.



Privacy Reviews

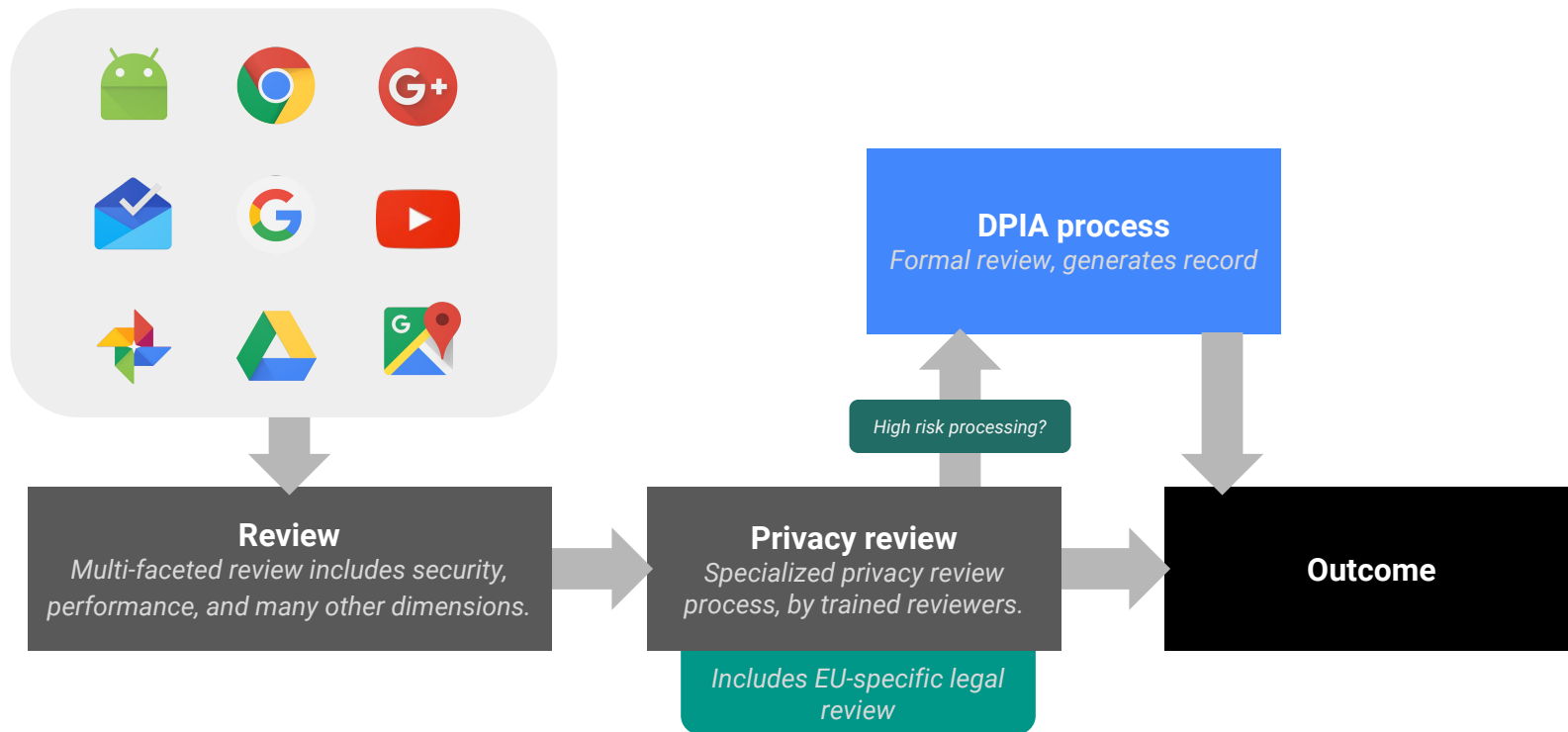
Privacy Working Groups (PWGs) partner with engineering teams throughout product development and conduct final launch reviews.

Each PWG team focuses on a product area (e.g. Chrome or Maps) or a horizontal privacy theme (e.g. biometrics or aggregation). **PWG members are experts in their specific domains, and they get specialized legal support.**

30

Privacy Working Groups
focused on product areas and
privacy concepts.

Privacy review model: DPIA process



Data Protection Impact Assessments

We're launching a DPIA template that will be a key deliverable of the review process for High Risk processing.

DPIAs will be reviewed by privacy engineering, legal counsel, product leadership, and the DPO as appropriate — building upon similar reviews we do today.



Description of the processing

High risk criteria

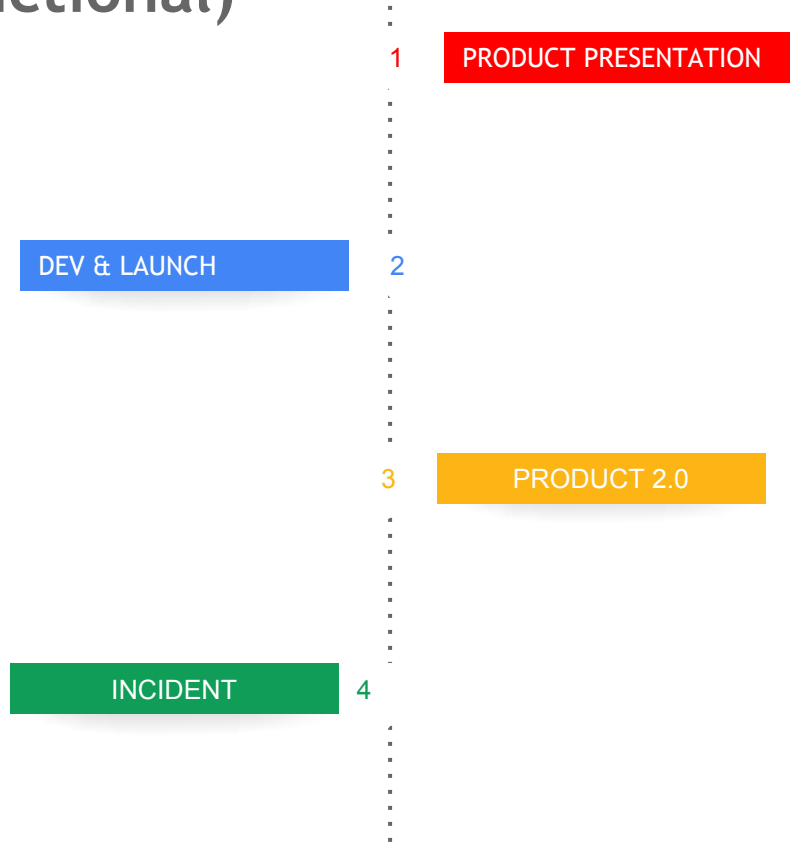
Risk analysis and mitigation

Stakeholder signoff

Part B: Fictional Case Study



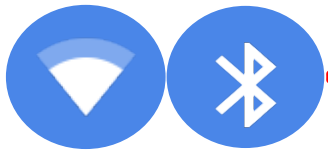
Case study (fictional)



BRUSH.ly
(fictional)



WiFi and Bluetooth enabled
to connect to phones

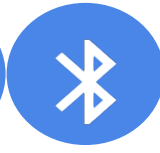


1

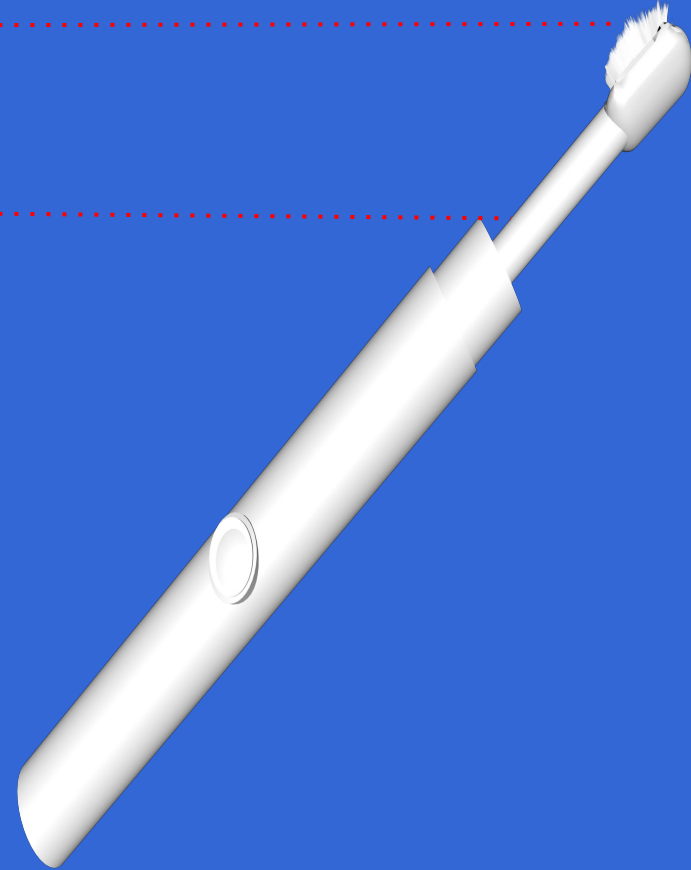
PRODUCT PRESENTATION



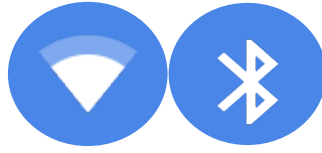
WiFi and Bluetooth enabled
to connect to phones



Companion mobile app to sync
with Brush.ly Account



WiFi and Bluetooth enabled
to connect to phones

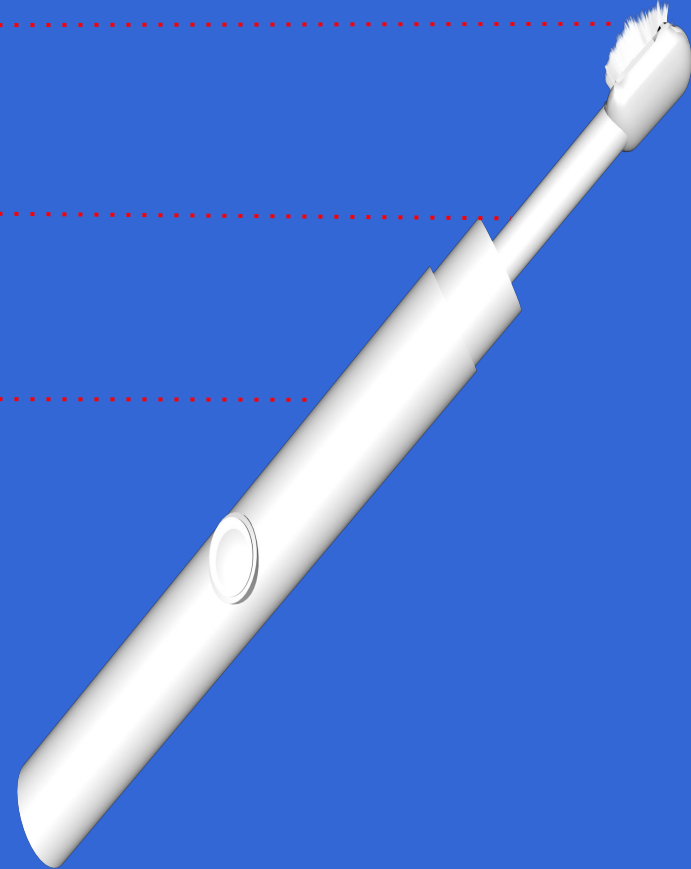


Companion mobile app to sync
with Brush.ly Account

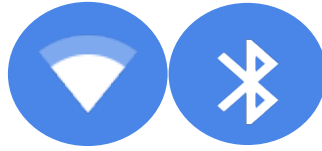


Keeps **detailed data** in local storage
about:

- Brush position
- Accelerometer and gyro readings of detailed movements
- Brushing time



WiFi and Bluetooth enabled
to connect to phones



Companion mobile app to sync
with Brush.ly Account

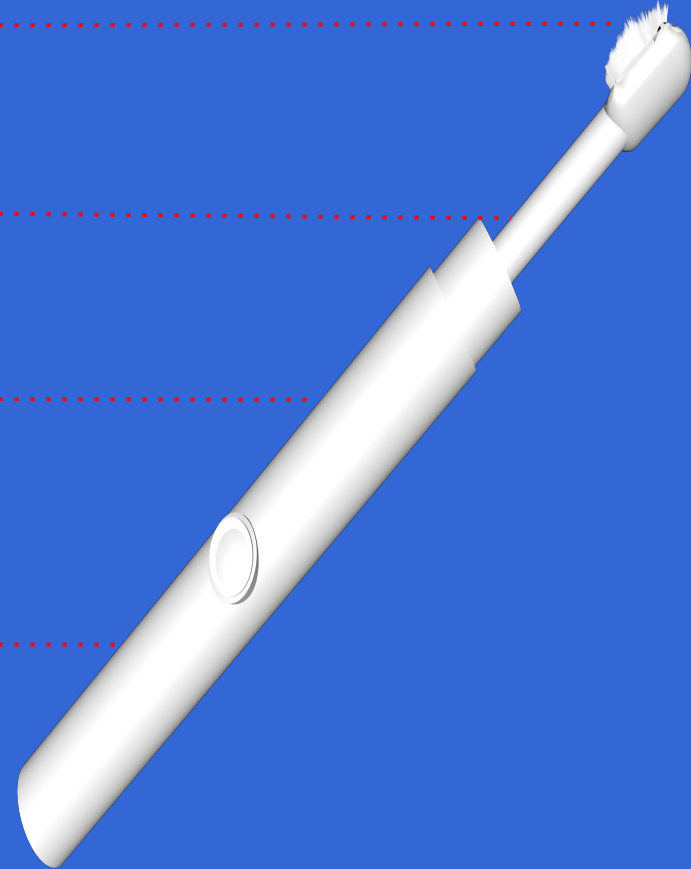


Keeps detailed data in local storage
about:

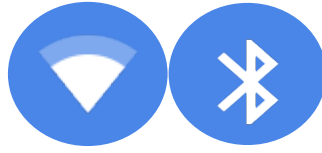
- Brush position
- Accelerometer and gyro readings of detailed movements
- Brushing time



Small screen displays brushing
statistics



WiFi and Bluetooth enabled
to connect to phones



Companion mobile app to sync
with Brush.ly Account



Keeps **detailed data** in local storage
about:

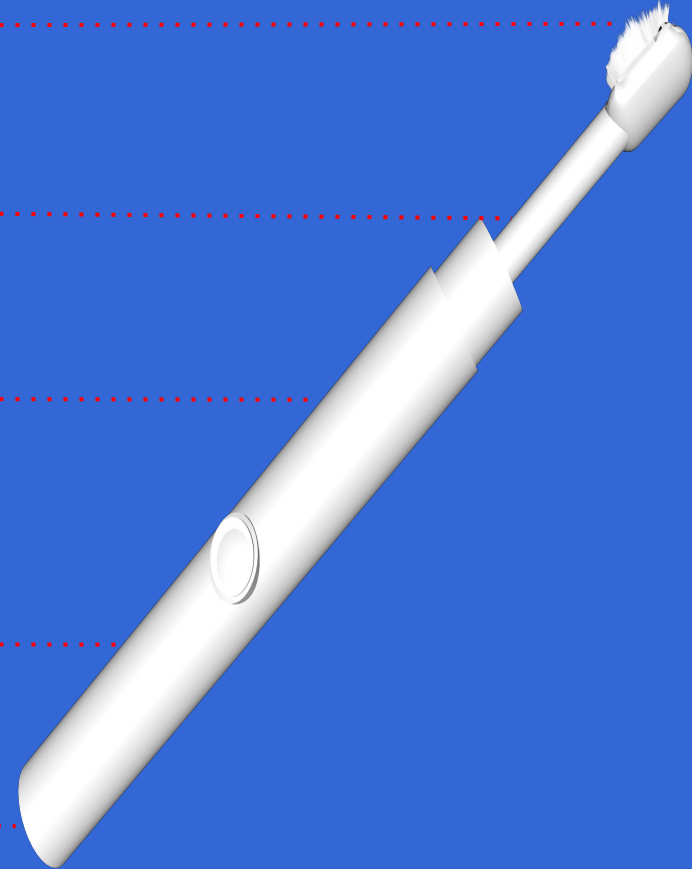
- Brush position
- Accelerometer and gyro readings
of detailed movements
- Brushing time



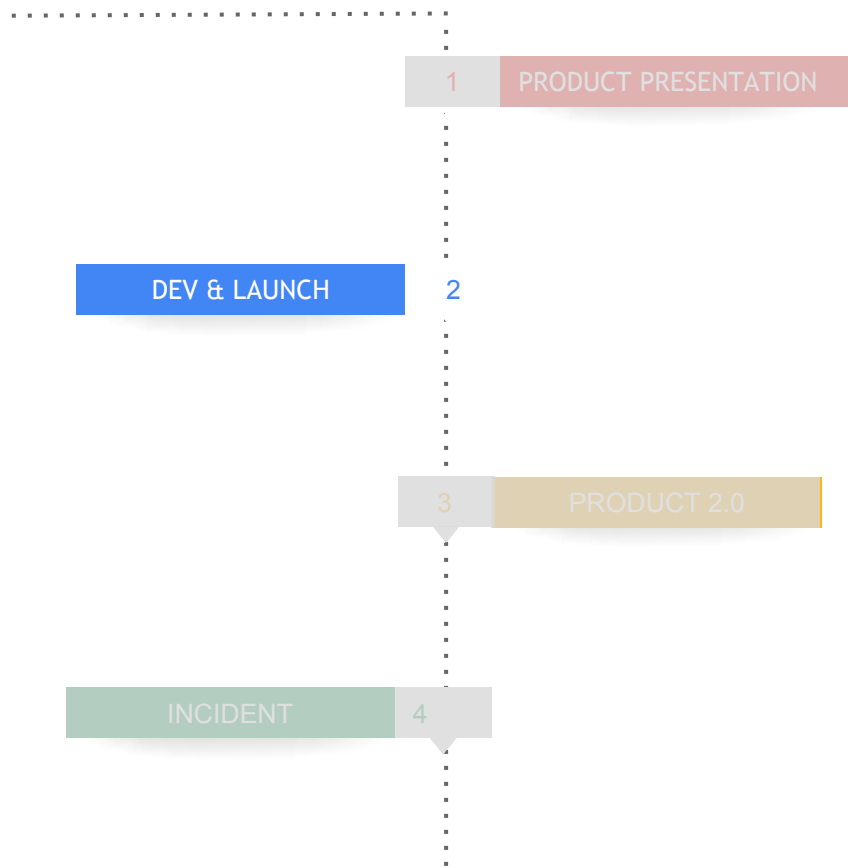
Small screen displays brushing
statistics



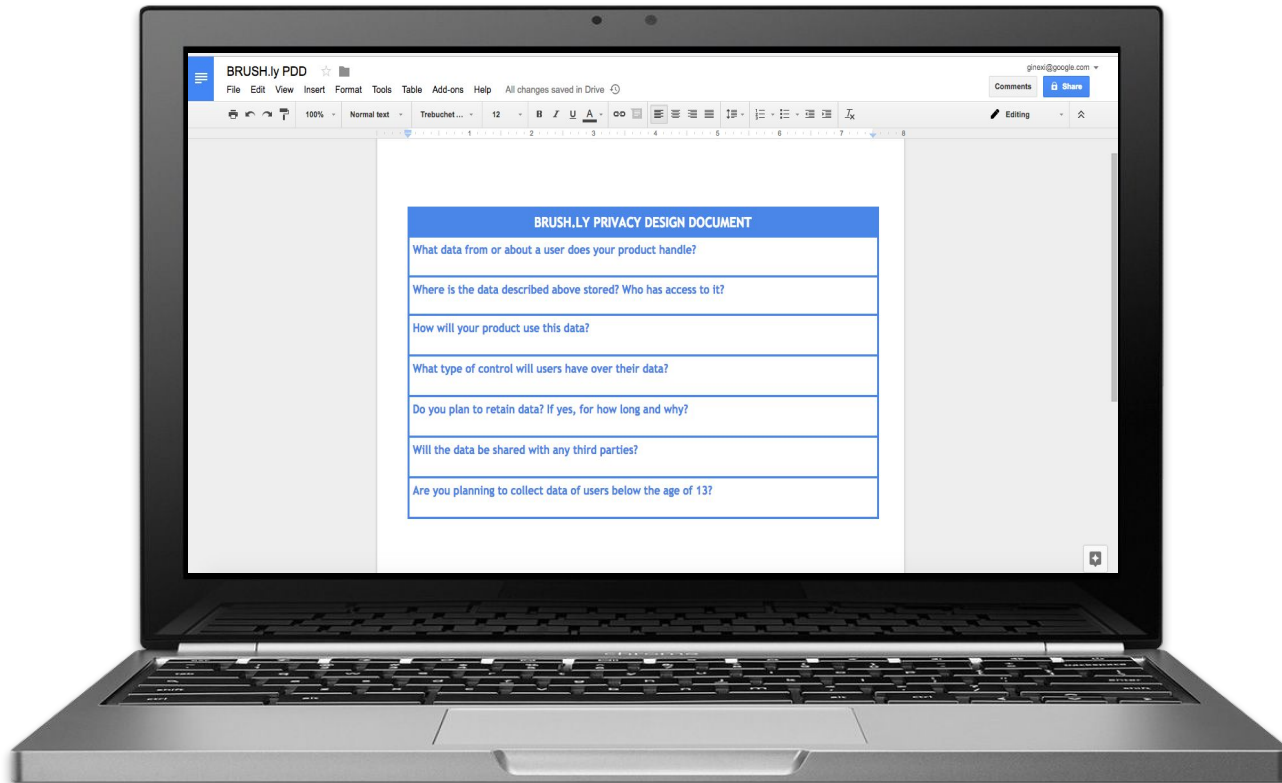
Research data will be made
available to researchers and
academics



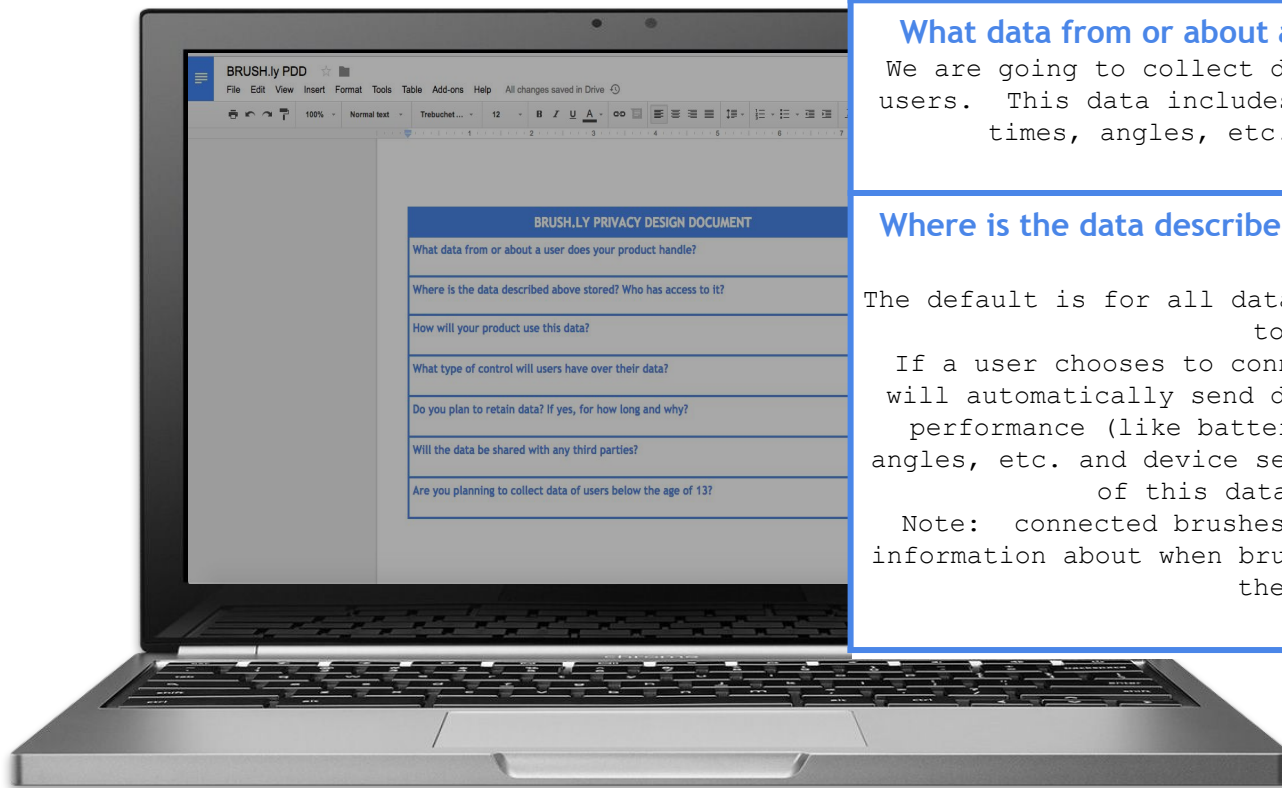
Roadmap



Privacy Design Document



Privacy Design Document



What data from or about a user does your product handle?

We are going to collect data from the toothbrush, not from users. This data includes: battery life, brushing speeds, times, angles, etc. and device serial number.

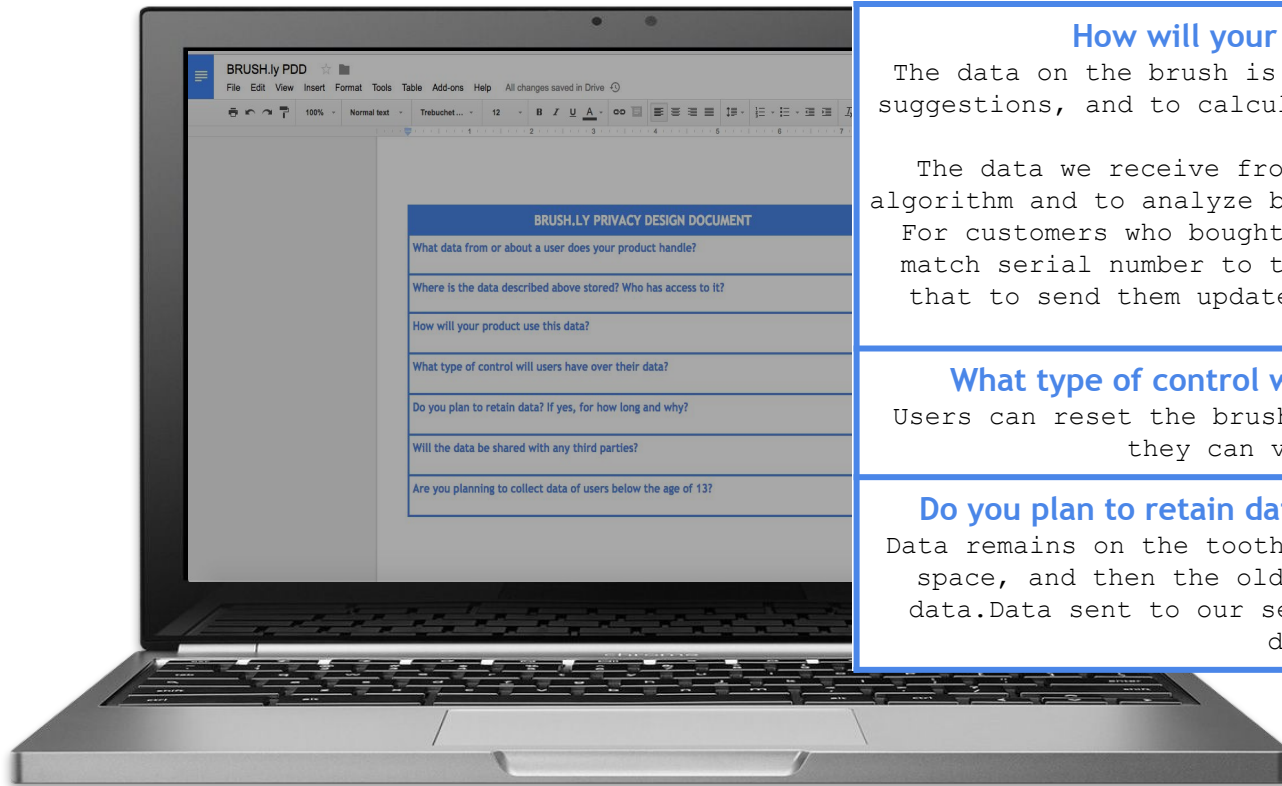
Where is the data described above stored? Who has access to it?

The default is for all data to be stored in the memory on the toothbrush.

If a user chooses to connect their brush with the app, we will automatically send data from the toothbrush about its performance (like battery life, brushing speeds, times, angles, etc. and device serial number) to our servers. None of this data is tied to a user.

Note: connected brushes can receive updates, and we log information about when brushes get updates and which updates they receive.

Privacy Design Document



How will your product use this data?

The data on the brush is used to provide the user tips and suggestions, and to calculate performance scores to show the user.

The data we receive from brushes is used to improve our algorithm and to analyze bugs or other issues with the brush. For customers who bought brushes directly from us, we can match serial number to their purchase information and use that to send them updates on the product and promotions.

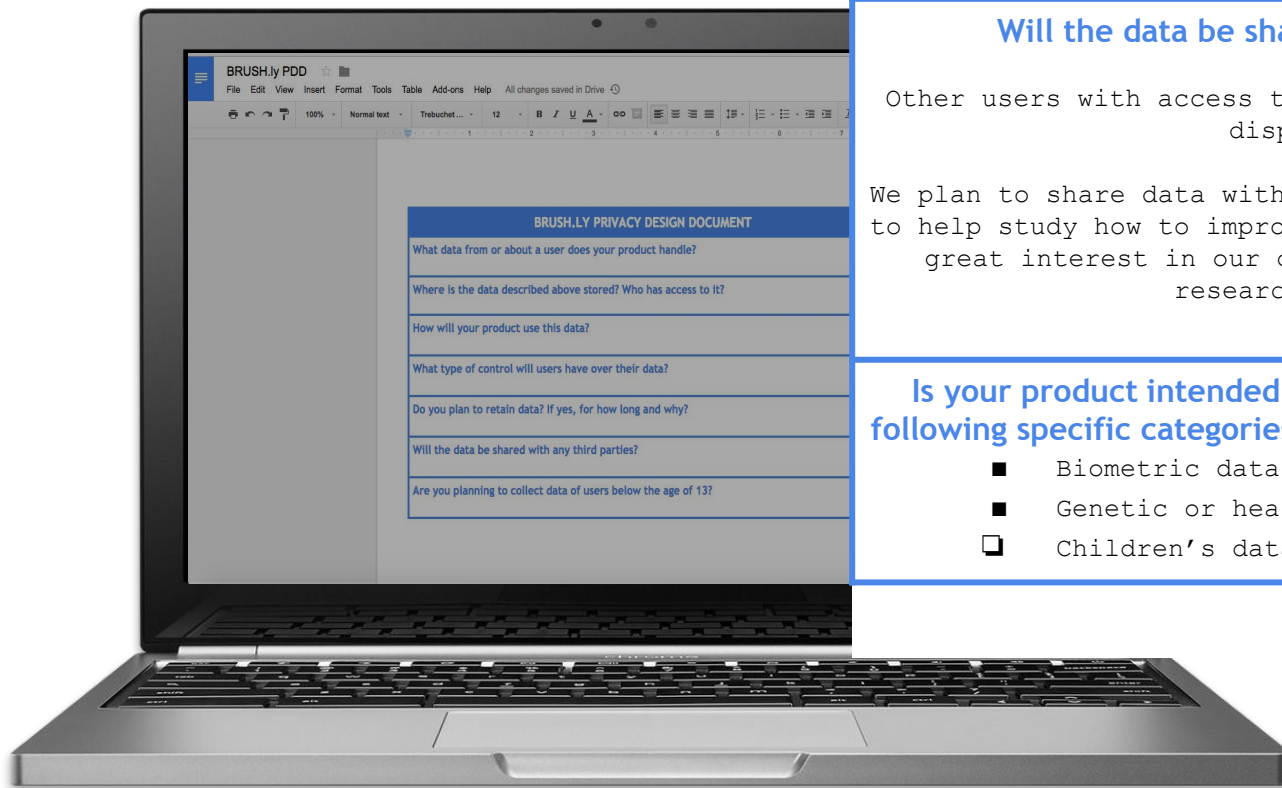
What type of control will users have over their data?

Users can reset the brush if they want to remove data, and they can view it in the app.

Do you plan to retain data? If yes, for how long and why?

Data remains on the toothbrush until the memory runs out of space, and then the oldest data is overwritten with new data. Data sent to our servers is kept until we decide to delete it.

Privacy Design Document



Will the data be shared with any third parties?

Other users with access to the brush could view data on the display screen.

We plan to share data with medical researchers and academics, to help study how to improve dental health. We know there is great interest in our data and have heard from several research labs already.

Is your product intended to collect and process any of the following specific categories of data (check all that may apply):

- ☒ Biometric data (e.g., fingerprints)
- ☒ Genetic or health information;
- ☐ Children's data

What does...

...a User Trust expert say about best practices?

- Transparency and control
- Communication about privacy
- Being trustworthy

...an Eng Expert say about best practices?

- Encryption
- Multi-users
- Hardware privacy vulnerabilities
- Sharing for research

...a Privacy Lawyer say about legal obligations?

- Notice & Consent
- Retention
- Accuracy in settings

Brush.ly Fact Sheet

WiFi and Bluetooth enabled to connect to phones



Companion mobile app to sync with Brush.ly Account



Keeps **detailed data** in local storage about:

- Brush position
- Accelerometer and gyro readings of detailed movements
- Brushing time

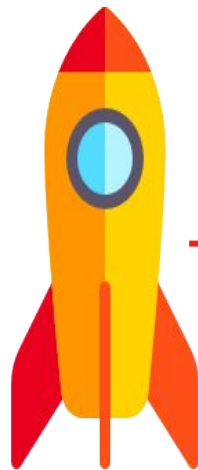


Small screen displays brushing statistics

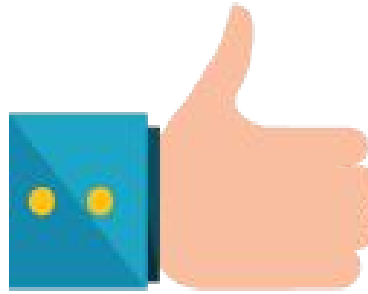


Research data will be made available to researchers and academics





Brush.ly launches

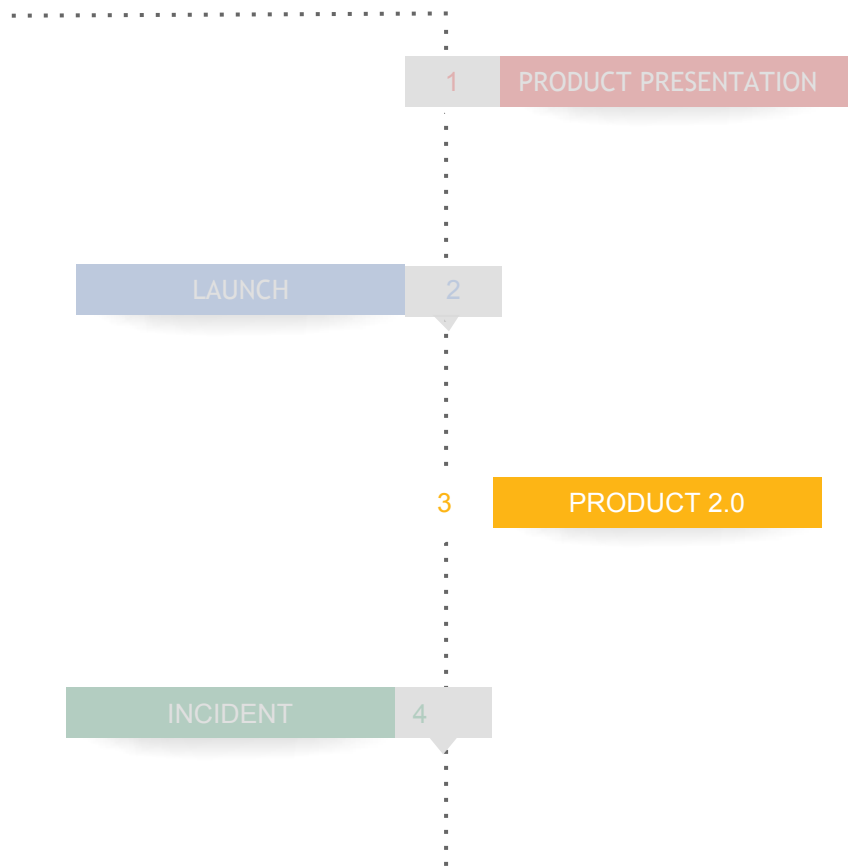


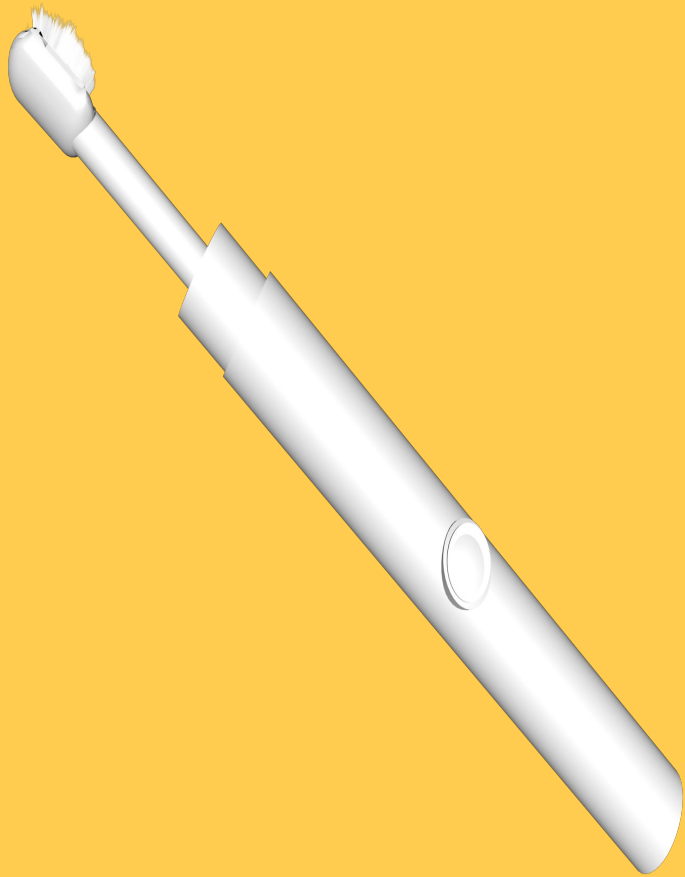
Users like it



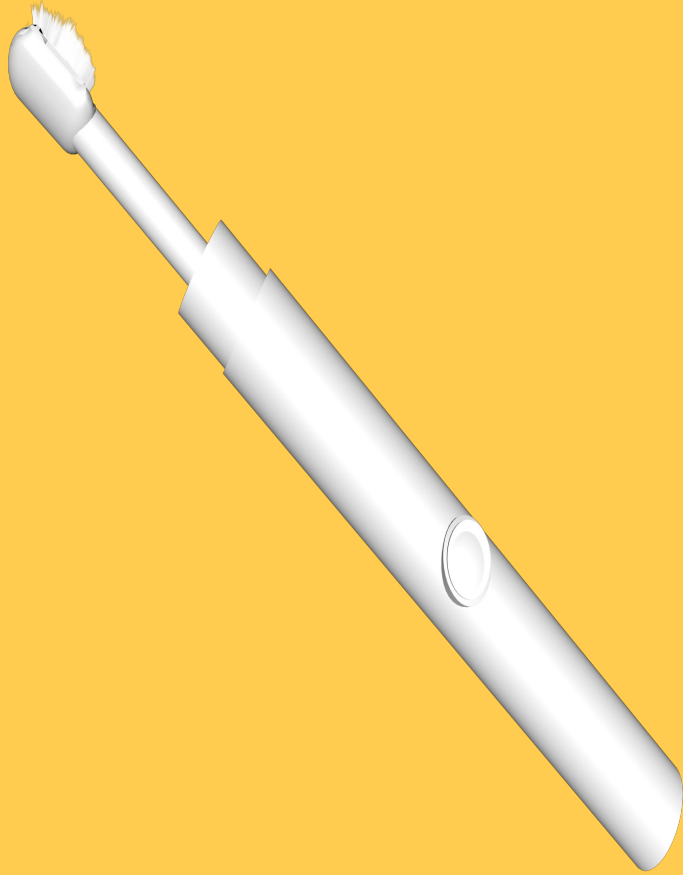
...3 months later...

Roadmap



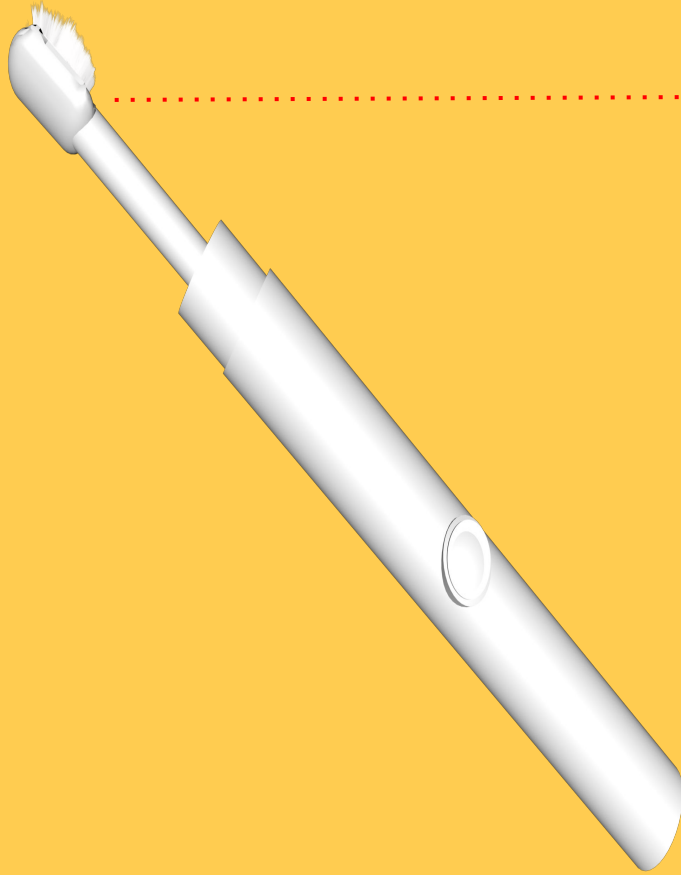


Super Smile
Brush.ly?
(fictional)

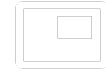


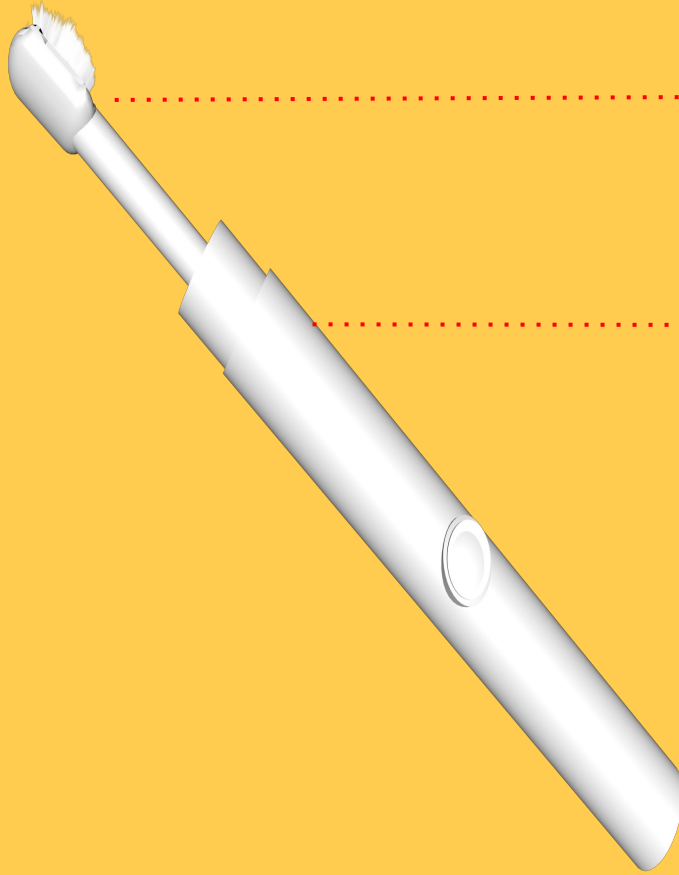
It will include all features of
Brush.ly





Sensors on brush can detect the presence of gum disease

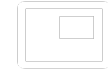


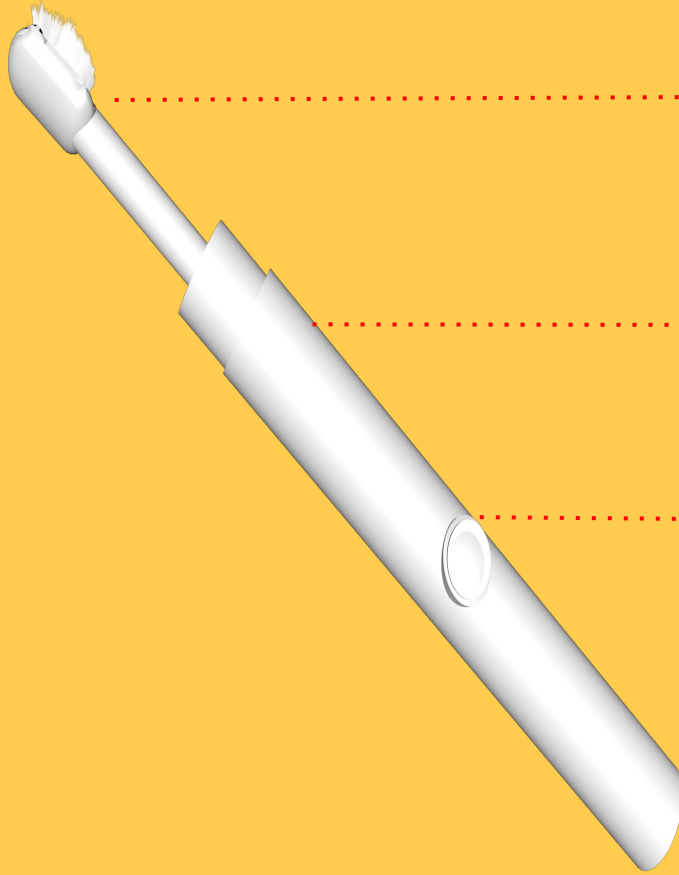


Sensors on brush can detect the presence of gum disease



GPS-enabled to detect user's location when using Brush.ly

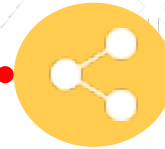




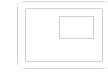
Sensors on brush can detect the presence of gum disease

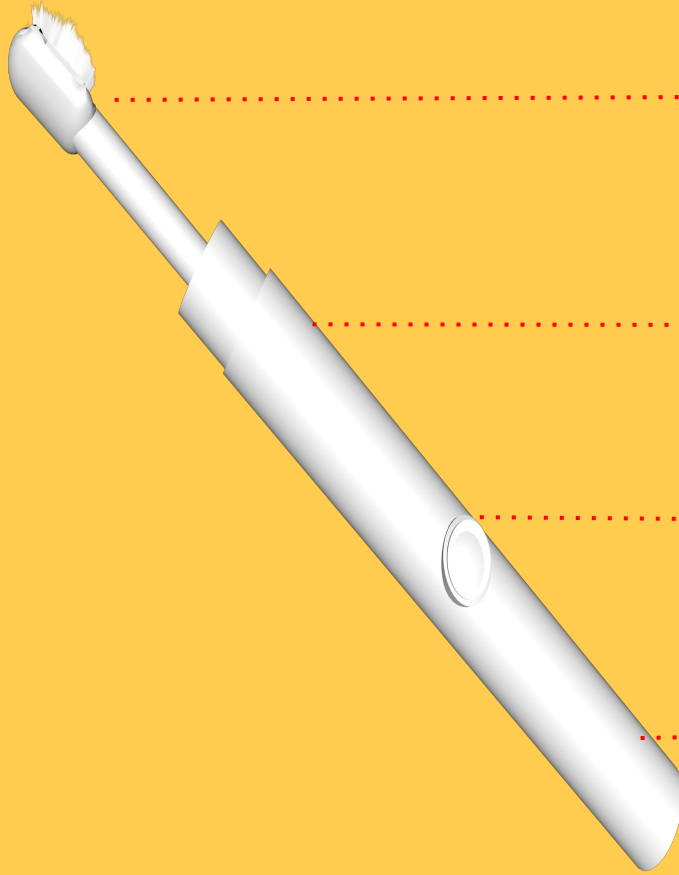


GPS-enabled to detect user's location when using Brush.ly



Users will be able to share their info with their dentists. Dentists can install a **Brush.ly App for Doctors**

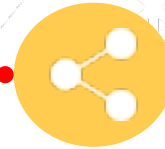




Sensors on brush can detect the presence of gum disease



GPS-enabled to detect user's location when using Brush.ly



Users will be able to share their info with their dentists. Dentists can install a **Brush.ly App for Doctors**

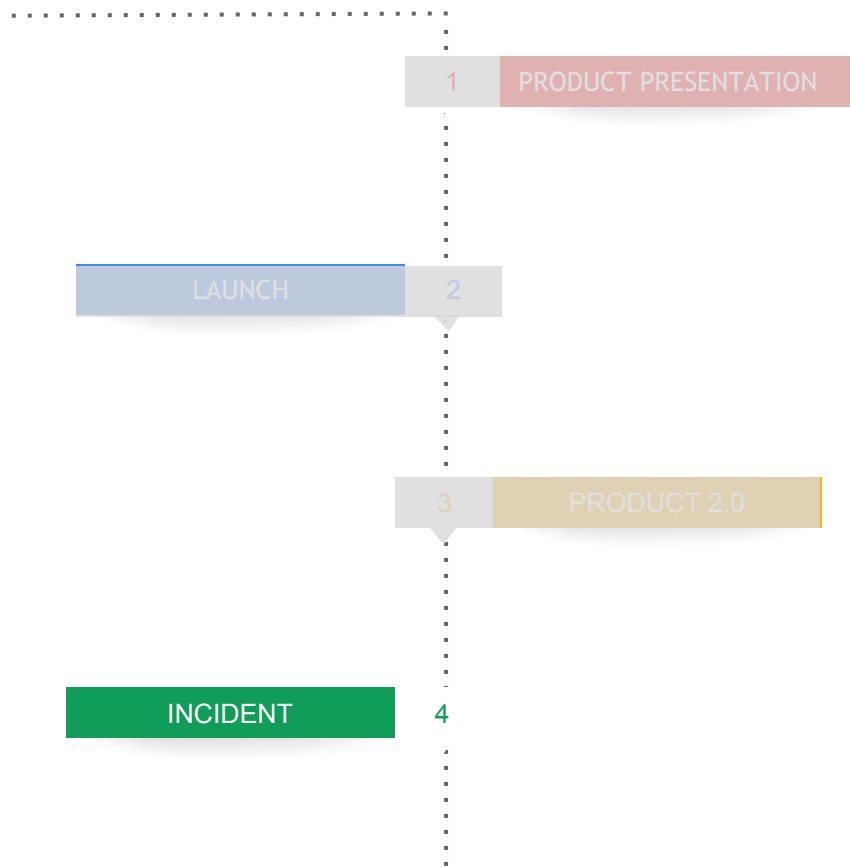


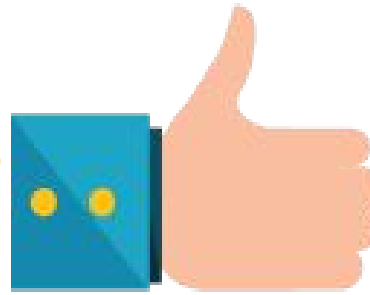
Special features for kids

Assessment of Super Smile Brush (fictional example)

Issue	User Trust	Legal	Privacy Eng
Health condition data is sensitive	How are you gaining user's trust to provide the data?	Opt-in consent and retention controls.	Storage and access restrictions.
Location data from a toothbrush	What if there are users who don't find this beneficial?	Privacy Policy allows using location, but notify users?	Shared device, so how do you avoid abuse of location data?
Sharing data with dentists	Can users remain aware of who has access to their data?	High Risk Processing considerations/processing conditions	How do you ensure the right doctor gets access to the right data?
Gathering data from kids	Do you understand how kids may interact differently with the brush?	Do you need parental consent?	What supervision features are in place for kids accounts?

Roadmap





Users like it



Incident!

What happened?



One of the engineering teams develops an **update to the companion app**



The new functionality allows users to book appointments with dentists **that have installed Brush.ly App for Doctors**



The update contains a **bug** in the code that unintentionally causes the name and email address of users who have used this feature to become available **to all the dentists** that have installed the companion Brush.ly App for Doctors

What happened?



One of the engineering teams develops an **update to the companion app**



The new functionality allows users to book appointments with dentists **that have installed Brush.ly App for Doctors**



The update contains a **bug** in the code that unintentionally causes the name and email address of users who have used this feature to become available **to all the dentists** that have installed the companion Brush.ly App for Doctors

What happened?



One of the engineering teams develops an **update to the companion app**



The new functionality allows users to book appointments with dentists **that have installed Brush.ly App for Doctors**



The update contains a **bug** in the code that unintentionally causes the name and email address of users who have used this feature to become available **to all the dentists** that have installed the companion Brush.ly App for Doctors



...a month later...

Fixing the bug



1-2 days of extra
engineering work
required

Fixing the bug



1-2 days of extra
engineering work
required



Extra week necessary for
formal review and
approval

Fixing the bug



1-2 days of extra engineering work required

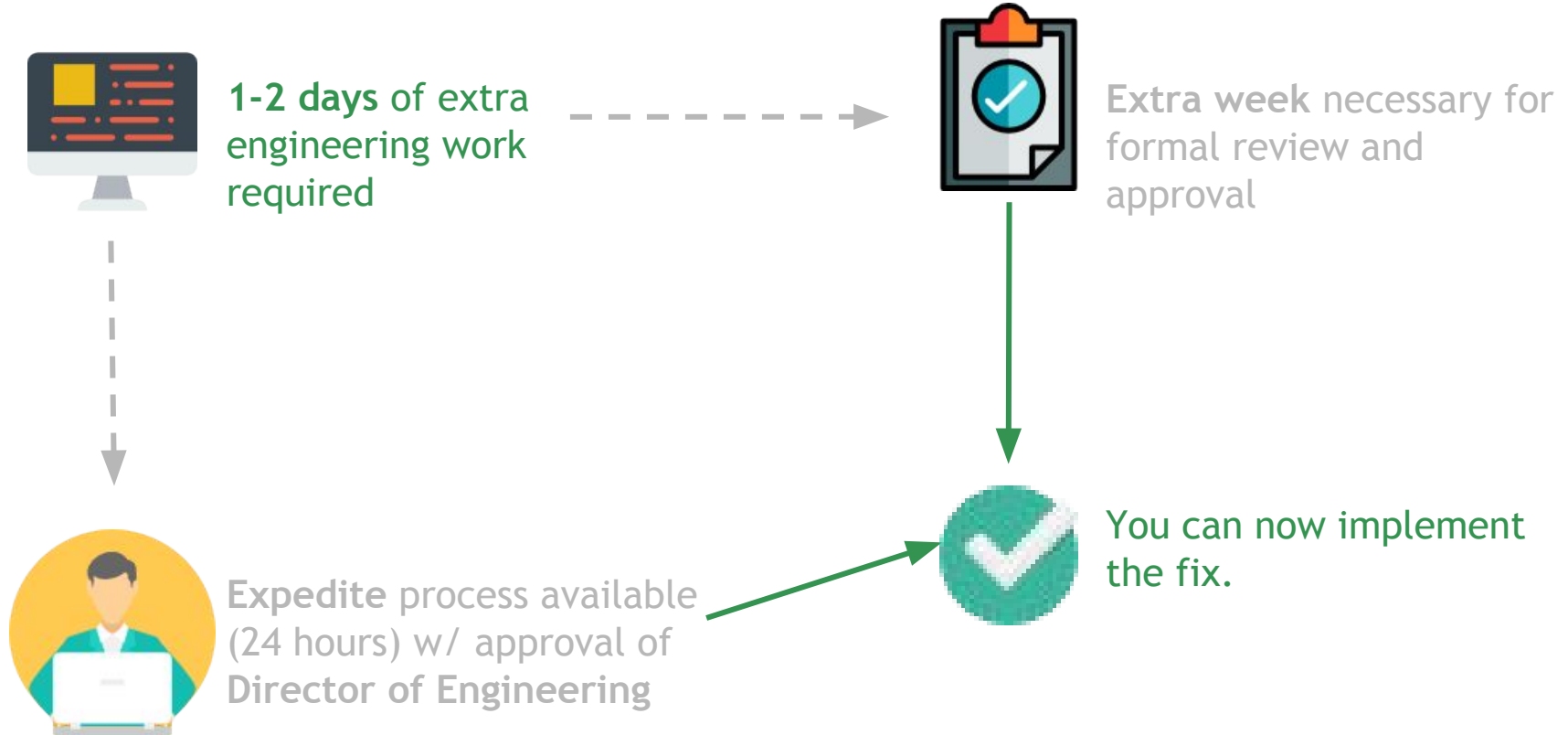


Extra week necessary for formal review and approval



Expedite process available (24 hours) w/ approval of Director of Engineering

Fixing the bug





What Privacy by Design issues are **highlighted** in this incident?



What Privacy by Design issues are **highlighted** in this incident?

What Privacy by Design issues come into play when **fixing the bug?**



Breach notification?

Thank You



Cyber Attack Tabletop

Preparing for and Managing Security Breaches

23 January 2018

Aaron Simpson
Hunton & Williams

asimpson@hunton.com
0207 220 5612

JoAnn Stonier
MasterCard

joann_stonier@mastercard.com

- New Requirements under Emerging Law
- Practical Impact of the New Requirements
- Tabletop Scenario

Requirements to notify the public and regulators began in the U.S. in 2003

- Notification requirements have now spread to more than 30 countries around the world
- Including new obligations in the EU under the GDPR

Even where there is no legal requirement to notify, significant cyber events tend to generate publicity

- And could require a stock exchange announcement

Significant changes coming with GDPR

- Personal data breach notification obligations
 - Must report breaches to:
 - Supervisory authority not later than 72 hours after having become aware, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons
 - Individuals without undue delay when the breach is likely to result in a high risk to the rights and freedoms of natural persons

Renegotiation of the ePrivacy Directive

Breaches result in significant direct and indirect business costs

- Notification-related costs
 - Legal and forensic investigation fees
 - Preparation and transmission of notifications
 - Public relations and other similar crisis management services
 - Establishment of a call center and other communications procedures
 - Fraud monitoring services
- Losses resulting from damage to reputation and client relationships
- Regulatory fines (up to €10M or 2% of global turnover under GDPR)
- Defending litigation and regulatory enforcement actions

Can be catastrophic:

- WannaCry: FT reports “WannaCry has permeated society to a point where it presents a threat to human life”
- TJX: \$256 million; Heartland Payment Services: \$140 million; Target \$162 million
- TalkTalk: £60 Million

Tabletop Scenario

- Timeframe: September 2018, GDPR is in force
- Children's online toy retailer based in Dublin called Acme Limited
- €250m in revenue
- Primary revenue source = sales in the EU.
- All revenue is generated by eCommerce sales
- Extensive supply chain throughout Europe

- Moderator: Aaron Simpson, Hunton & Williams
- Counsel: JoAnn Stonier, MasterCard

- Cybersecurity risks are factored into Acme's broader risk management portfolio
- The Company's approach can be summed up in the following statement:
 - *"We're a toy company -- not a tech company. We look at cyber as we look at other risks: there is a certain amount of pain we are willing to absorb before we will invest an incremental euro."*

- One of Acme's competitors in the online toy market is making headlines for being hacked.
- This corresponds with a noticeable uptick across the eCommerce space in sophisticated targeted cyberattacks.
- Acme recently ran an Anti-Virus update for its network -- resulted in discovery of malware on an administrator's workstation.
- Acme's security team forensically analysed the workstation and unearthed a suspicious file in a temporary directory.

- Acme decides to engage a forensic consultant to perform a detailed forensic investigation.
- The forensic traces the source of the initial infection to a small toy supplier in Germany.
- An attacker embedded a piece of malware into an Excel worksheet that was exchanged between Acme and the German supplier during the ordering process.
- Further investigation shows that the attacker has gained access to Acme's back-end customer database
 - Includes 1m customer records containing contact information, payment information and information about past purchases that provide Acme with the ability to selectively market based on the age and gender of the customer's child
- Management does not believe anyone outside of Acme or the German toy supplier is aware the incident has occurred
 - The GC believes there may be breach notification obligations under the GDPR
 - The Board is asking questions and there are very limited (and tentative) answers available

- Nevertheless, Acme's internal PR team receives a call from an blogger who is notorious for covering (and breaking) stories regarding cyber incidents.
- The blogger asks Acme for comment about their recent hack.
- The blogger says he will post a story on the issue within 12 hours, with or without a comment from Acme.
 - Some senior managers want to issue a press release and get in front of the story before Acme is named in the media.

- The blogger has published his story and the media is beginning to disseminate it.
- The Irish Times and the London tabloids have picked up the story.
- Some aspects of the stories as they are being reported are clearly inaccurate.
- The CEO and the internal comms team have received numerous calls from national media asking the company for a statement.
- Employees have begun to reach out to HR with questions of their own.
- The Board has requested another update.

* * *

- Leverage your Article 30 inventories to understand your data flows in the security context
- Maintain incident response plan and prepare data breach toolkit
 - Plan should also include retention of relevant external advisors (legal, forensic, PR/comms, call centres)
- Determine internal roles and responsibilities, governance and channels of communications
- Stress test the incident response plan and governance structure through tabletop exercises
- Continually assess status of technical and organisational protections for data
- Manage vendor risks
- Manage insider risks
- Train employees and increase awareness
- Assess cyber insurance

Questions?



Peer Review

Design Jam Team | CIPL | Feb 22nd



Elaine Montgomery

Design Manager, Facebook

Chris Downs

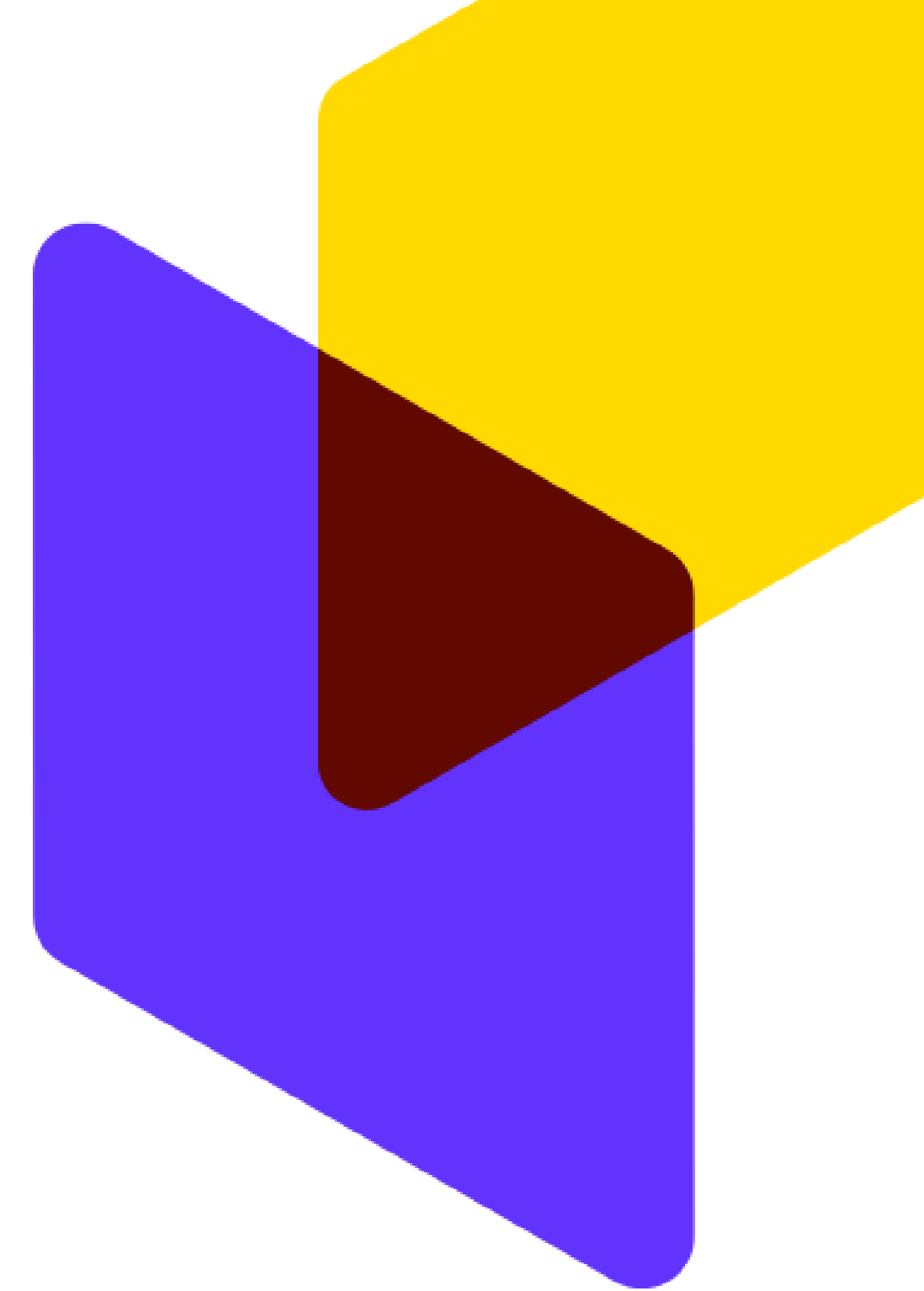
Managing Director, Normally



Design Exercise – Peer Review

We'll spend the next 30 mins doing a design exercise.

We use this exercise (and others) in 1-day Design Jams where we bring together industry, design, policy, legal and regulators to co-create new user experiences for trust, transparency and control.



What constitutes a timely and meaningful notice?

We use the 'Peer Review' exercise to learn how other businesses have approached privacy & consent notices.

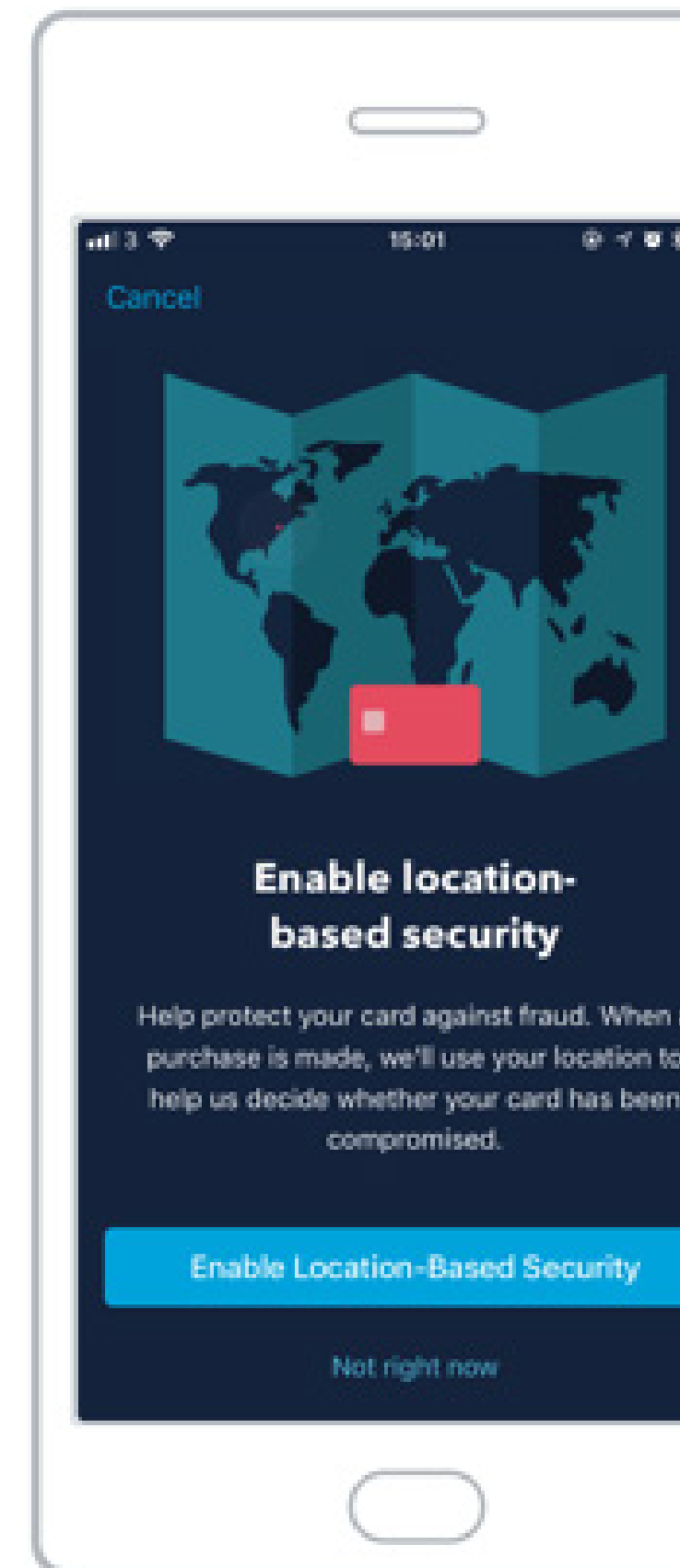
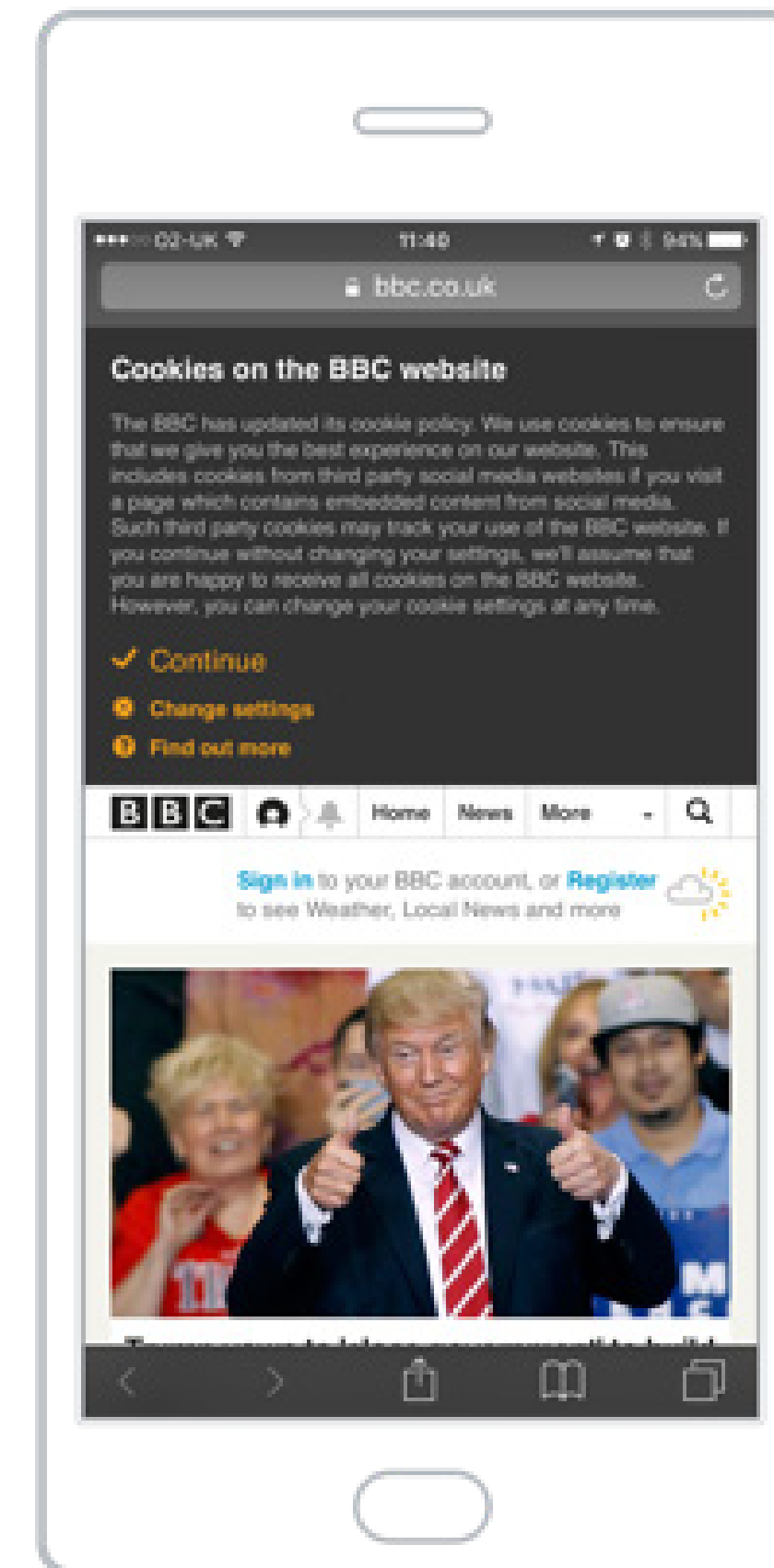
You will review 6 different business example to decide which are the most effective.



Is it clear?

Consider how well the following design elements are used to provide clear & transparent notice.

- **Language** (is it transparent, human & clear)
- **Visual design** (accentuating important info)
- **Interaction** (when the user sees it)



Rank the Notices

In your team of 3, discuss and then draw a line from each app to where you think it sits on the axis.

Peer Review (page 1) Rank Notices

Review the accompanying notice examples on page 2 & 3 to decide which are the most effective. Draw a line from each thumbnail to its position on the "More-Less Effective" axis.

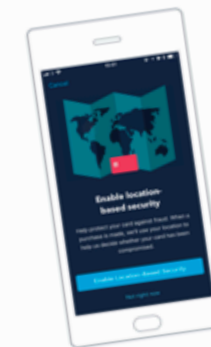
Consider how language, visual design and interaction are used to communicate clearly and provide transparency.

LESS EFFECTIVE

MORE EFFECTIVE



BBC



Monzo



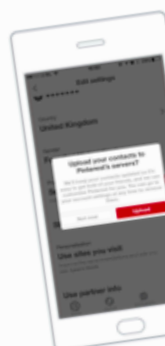
Trello



OpenTable



Barclays Pingit



Pinter



What now?

Look under your chairs
for a **clipboard of
material & instructions**



Divide into **groups of
three** with the people
sitting next to you



You'll have **15 mins** for
this exercise - Let's start!



What did we learn?

- There's no single correct answer
- When the notice appears, is as important as the notice itself
- Build trust with people over time
- Explain the value exchange of data



The background features several large, stylized geometric shapes, primarily triangles and polygons, in shades of teal, yellow, green, and pink. These shapes are arranged in a way that they appear to be floating or layered around the central text. Some shapes are solid colors, while others have internal divisions or gradients.

Get in touch!

Contact **adambargroff@fb.com** to discuss beta access to our toolkit and becoming a partner.

Alternatively, join our mailing list at

www.fb.me/designjam

Workshop by the Centre for Information Policy Leadership in collaboration with the Office of
the Data Protection Commissioner of Ireland

How can Organisations Deliver Accountability under the GDPR

The Printworks, Dublin Castle, Dame St,
Dublin 2, Republic of Ireland
23 January 2018 | 9:00-17:45

Session IV: Individual Rights & Complaint Handling

Rob Corbet,
Head of Technology & Innovation, Arthur Cox

Ireland Law Firm of the Year 2017
Chambers Europe Awards

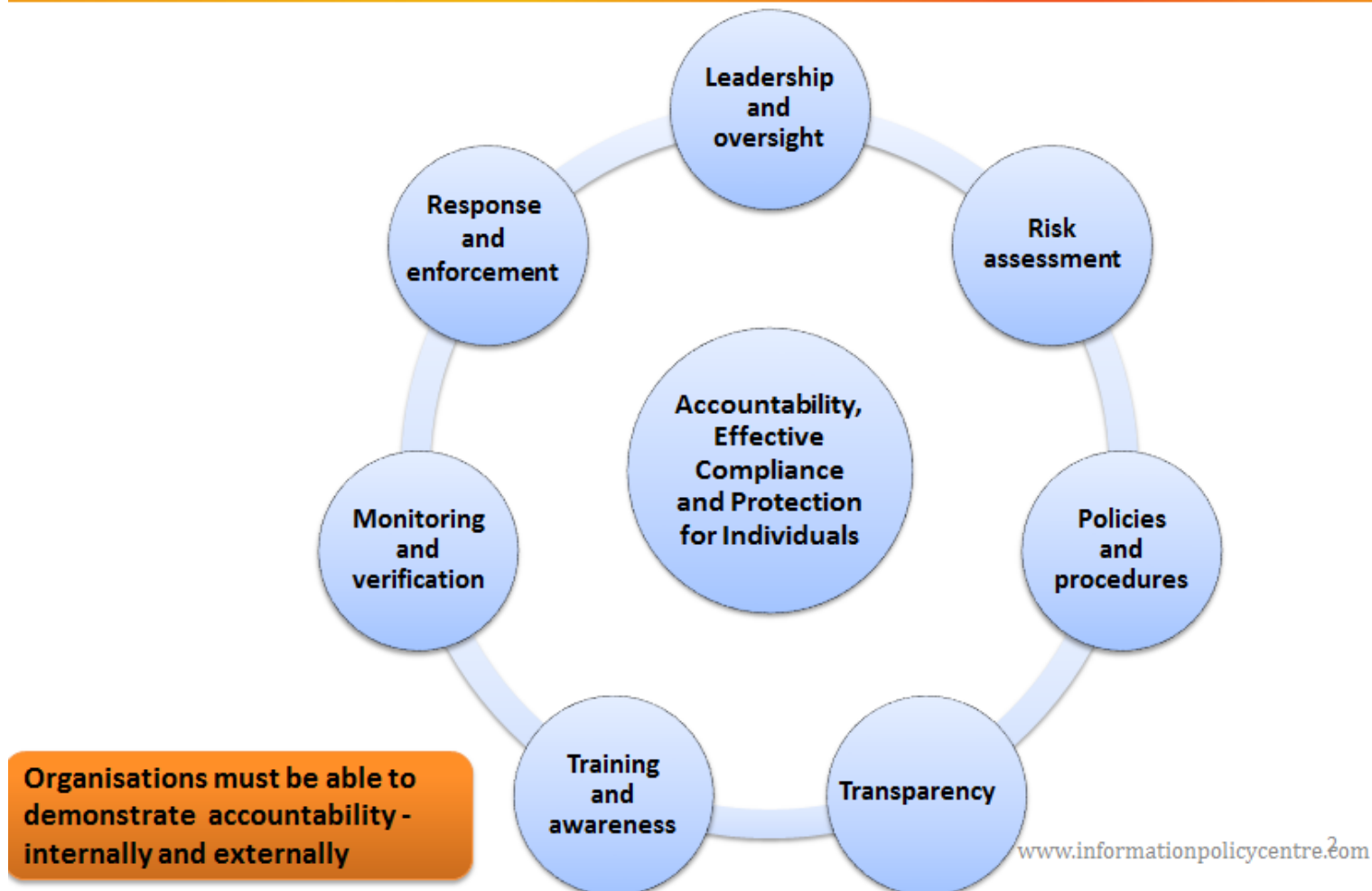
Best Firm in Ireland 2017
Europe Women in Business Law Awards

Ireland Law Firm of the Year 2016
International Financial Law Review (IFLR) Europe Awards

Ireland Law Firm of the Year 2016
Who's Who Legal

ARTHUR COX

CIPL Accountability Matrix



Data Subjects' Rights

DPAs 1988 and 2003 v GDPR

Existing Rights

- Right of Access
- Right to Object
- Right of Rectification
- Right to Erasure
- Automated Decision Making (including Profiling)

New Rights

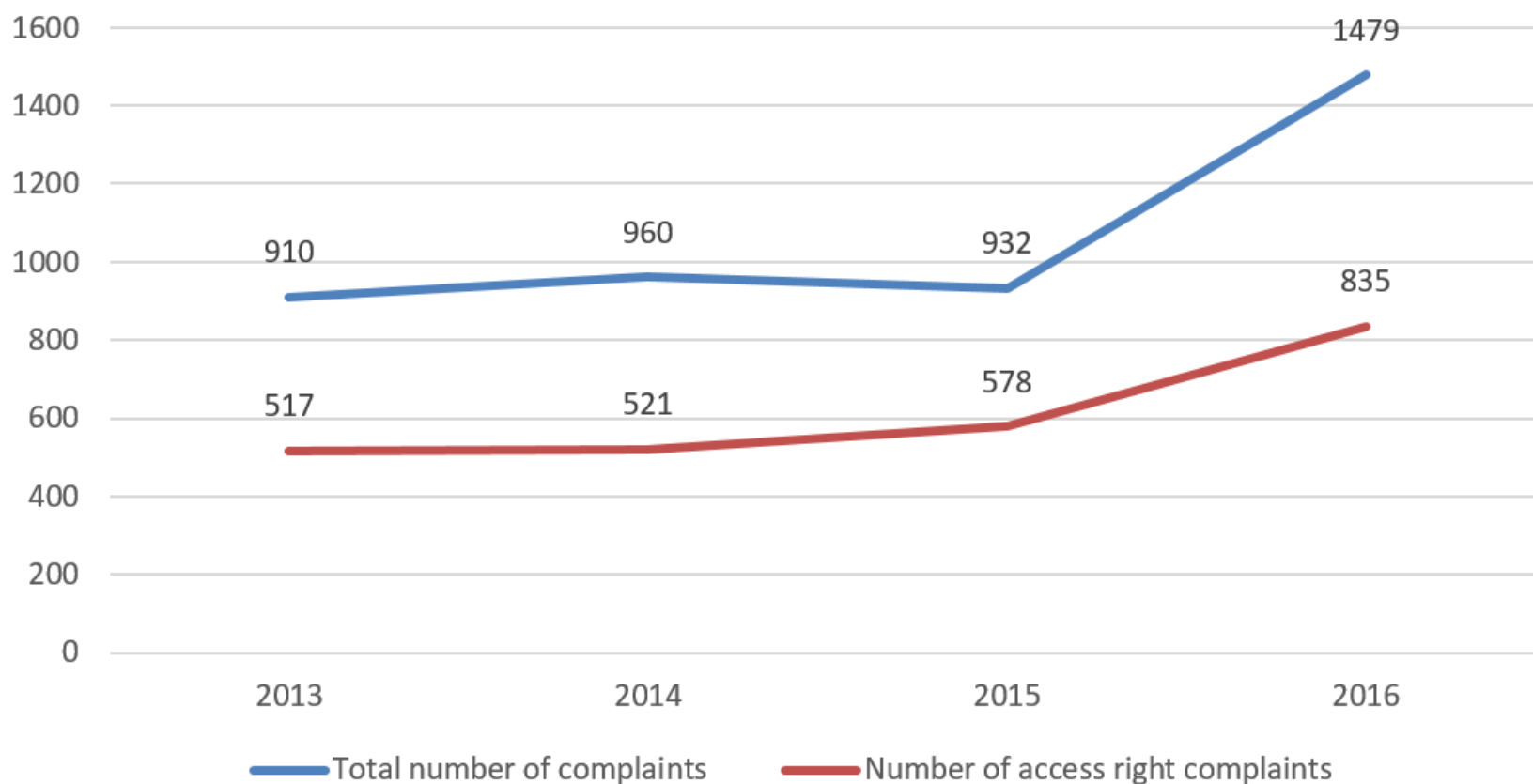
- Right of Restriction
- Data Portability

DSARs: DPAs v GDPR

	DPAs	GDPR
Scope	Purpose, categories, recipients, logic of automated decision making, if the bases of any decision likely to significantly affect data subject	Purpose, categories, recipients, storage period, right of rectification/erasure, right to lodge complaint, source , logic of automated decision making and its consequences
Timeline	40 days	1 month , extendable to a further 2 months
Cost	Reasonable fee (max. €6.35)	Free unless requests manifestly unfounded or excessive
Form	“Intelligible Form”	If request provided in electronic form, must provide response in electronic form

DSARs > 50% of Total DPC Complaints

Source - ODPC Annual Reports 2013 - 2016



ODPC Expectations

‘The Article 30 obligation to document data processing operations is not a pen-pushing exercise. It’s all about becoming aware. And compliance can only flow from awareness.’

Commissioner Helen Dixon
Privacy Laws and Business Conference



‘Accountability is the essence of the GDPR. Organisations must make the investment to ensure they take enhanced responsibility for personal data processing using a risk-based approach. Equally they must be capable of demonstrating that accountability to data subjects and to regulators.’

Commissioner Helen Dixon
Privacy Laws and Business Conference



- Art 5(2) - Accountability Principle (new)
- Art 30 – Records of Processing Activities (new)
- Art 32 – “Appropriate technical and organisational measures” (new)
- Art 35 – DPIAs for high risk processing (new)
- But remember Art 24 – Risk based approach (new)

Thank You

Rob Corbet leads our Technology & Innovation Group. His practice is focused on the protection and commercial exploitation of technology, data and intellectual property.



Email: rob.corbet@arthurcox.com

DUBLIN

Ten Earlsfort Terrace
Dublin 2
D02 T380
Ireland

t: +353 1 9201000
f: +353 1 920 1020
e: dublin@arthurcox.com

BELFAST

Victoria House
Gloucester Street
Belfast
BT1 4LS

t: +44 28 9023 0007
f: +44 28 9023 3464
e: belfast@arthurcox.com

LONDON

12 Gough Square
London
EC4A 3DWE
United Kingdom

t: +44 207 832 0200
f: +44 207 832 0201
e: london@arthurcox.com

NEW YORK

One Rockefeller Plaza
15th Floor
New York NY10020
USA

t: +1 212 782 3294
f: +1 212 782 3295
e: newyork@arthurcox.com

SILICON VALLEY

800 West El Camino Real
Suite 180, Mountain View
California 94040
USA

t: +1 650 943 2330
f: +1 650 962 1188
e: siliconvalley@arthurcox.com



Experts in Data Protection, Compliance & Training.



Data Subject Access Requests under GDPR

A practical roadmap

23 January 2018

Kate Colleary





Current Regime Vs GDPR

Subject to certain exceptions, individuals are entitled, on **written** request, to:

- Be told whether data controller holds data concerning the data subject (**S3 DPA**)
 - A copy of their personal data – **S4 DPA** (40 days to comply – one month under Art 12(3) GDPR)
 - Have any inaccurate or misleading data amended or erased (**S6 DPA**)
-
- Data controller may charge up to €6.35 (access only) – not a grounds for delaying commencing process of search (fee being removed by Art 12(5) GDPR)
 - Article 15 GDPR; Art 23 exemptions
 - Article 12(3) time limits
 - Significant increase in DSARs likely post-GDPR and issue of fines (€10m/2%) & litigation



A PERFECT STORM





DSAR PROCESS

Creating a DSAR Process- steps:

- Verification
- Search
- Review, extract & collate and
- Response

Thema International case (Clarke J) 2011 IEHC (discovery case)



Creating a DSAR Process

Steps and actions

Verification and log

- Data Subject ID verification procedure
- DSAR Log & diary system
- Monitoring of social media/emails
- DS Portal?

•Search

- Review of systems
- Centralised data storage
- Access to data for DPO team

Review

- Protocol for review
- Extract & collate
- Exemptions
- SI's
- Technology and appropriate systems NB
- 3rd party consent
- Clinical sign off (medical records)

Respond

- Comply with timeline
- Template schedules
- Template letters to DS
- Retain log of requests



Getting Started on Creating a Process

Review Systems & upgrade if necessary

- ☐ Identify where data is stored
- ☐ Data inventory
- ☐ Consider whether appropriate systems are in place for larger volume of requests in a shorter period of time
- ☐ Consider centralising where possible
- ☐ Consider Recital 63 – make personal data available via portal

Draft / amend processes

- ☐ Draft DSAR process – consider necessary steps (including 3rd party consent & medical sign off if necessary)
- ☐ Diary Management process
- ☐ Train DPO staff in all processes & all staff - awareness raising

Draft / amend templates

- ☐ Request Form
- ☐ DSAR acknowledgment
- ☐ Internal notifications/forms
- ☐ Internal sign offs
- ☐ Schedules
- ☐ Response letter



Kate Colleary
Co-Founder & Director

T: +353 19058695 E: kcolary@frontierprivacy.com W: www.frontierprivacy.com

*This presentation contains general information. This presentation is not intended to constitute legal advice and therefore should not be relied on as such.