Personal Data Receipts

Making Consent Work
August 31th
Mydata 2017, Helsinki

Michele Nati
Lead Technologist Personal Data and Trust

Digital Catapult, London
@michelenati
https://www.linkedin.com/in/michelenati/
The Personal Data Economy: The opportunity

• Personal Data is driving organizations digital transformation (Source: DCMS)
  
  241£ (66£ UK) billion growth between 2015-2020
  11% increase in customers, 10% new opportunities

• … with main sectors being digital health and digital manufacturing

  and benefits for both businesses and consumers (due to more personalization, prevention, automation)

  (Source: BCG) Digital Health estimated growth: $54Bn -> $213Bn, $8Bn -> $112Bn
  (Source: BCG) Digital Manufacturing estimated growth: $1Bn -> $6Bn, $11Bn -> $52Bn
The Personal Data Economy: The risks

• But hidden business models and lack of transparency are hindering this growth

  (Source: MEF) 53% of consumers report lack of control on how their data are used
  (Source: Data Protection Eurobarometer) Only 1 in 5 Consumers read privacy statement: 2000 words long, 10 minutes avg reading time
  (Source: MEF) 40% of mobile app users identify lack of trust as cause to abandon a service

• Savvy consumers demands for trustworthy apps (33%), with simple privacy statements
Transparency: Consumers pain points

Lie & Agree
Long, complex, lack of clarity and information (in particular for mobile apps)

TaCs
Agree and Forget

Information Notice
(Pre-service) Notice should be:
- Clear, concise and transparent
- Clear and plain language
- Highlight purpose, store, retention, individual rights

Information Receipt
(During-service) Individual rights:
- Track of shared data
- Manage consent
- Subject Access Request
- Remove data
- Data portability

We need best practices to increase transparency and control
GDPR:
Innovation opportunities

First step: Transparency
Savvy consumers demand
- Simple privacy statements
- Clarity on collected data and access to them
- Better user experience

- Transparency (Article 12-14, Information notice)
- Accountability (Article 4 and 7, Consent)
- Level of Control (Article 17-19, Data erasure and portability)
The Challenge

**Problem Statement:** How to increase consumers’ trust and businesses’ transparency by developing a GDPR compliant solution that takes into account the user experience and help to reduce consumers pain points and organizations compliance burden related to the provisioning of digital services using personal data?

**Personal Data Receipts (PDRs),** a human-readable record summarizing in a simple and clear way what personal data an organization is collecting about an individual, for what purpose, how they are stored and for how long and if any third party sharing is allowed.
Testing our hypothesis

- Understanding consumers barriers and what transparency means for them (TaCs pain points)
- Mocking up of a receipt, interviews, user-centric design, prototyping, measuring
- Findings: transparent, clear and concise summary of collected data, build trust

This is a summary of how your data is used within our organisation:

<table>
<thead>
<tr>
<th>CONTENT</th>
<th>STORAGE</th>
</tr>
</thead>
</table>
| Name, Email, Address, City, Postcode, Phone number | Your data:  
| Purpose: Health & Safety Issues, Our centre metrics |  
| Sharing: We do not share your data with third parties. |  

If you have any questions or doubts about how your information is used by us, please feel free to get in touch with this as receipt at datacontroller@organisationx.co.uk.
Digital Catapult PDRs

Multi-disciplinary team:
- UX Lead
- Marketing experts
- Lawyer
- Lead Tech

Beyond Consent:
According to DPA, consent is not required for:

a) the “legitimate interests” of the data controller so long as they do not override the fundamental rights of the data subject;

b) data that it is necessary to collect or process to fulfill a contract the data subject asked to enter

- PDRs are a super-set of consent receipt
- First full transparency, then control

Is there any privacy risk?
- For individuals?
- For businesses?
PIA and Privacy by Design performed

- 4 weeks development/integration
- Including data discovery phase
Digital Catapult PDRs implementation

Some note about privacy:
- No new personal information is created; nor passed and stored across different systems
- Secure meta-data communication
- Pseudonyms to link PDRs and users
- PDRs only sent the first time, with random delay, to avoid traceability
- Audit trail: including PDR version for maintain consistency (in case of Privacy Policy change)
PDRs: the benefits

Individuals (Savvy consumers):
• Privacy policies become human and simplified
• Track and control on personal data sharing is simplified (and possible!!)
• Reassurance that data will not end in the wrong hands is possible (3rd party sharing highlighted)

Services and apps become more trustworthy and more data are shared

Organizations:
• Attitude to personal data become user-centric
• Open new personal comm channel with their uses

Consumers trust increases and churn is avoided, while more data are accessed
GDPR compliance

- **Article 12-14, Information notice**
  - Use of icons and simple text to explain: what, how and for what purpose
  - *(could be extended to target different demographic groups)*

- **Article 4 and 7, Consent**
  - Provides a record for both individual and organization
  - Includes data collected under consent
  - *(currently only in human-readable format; could be extended with link to consent management platforms)*

- **Article 17-19, Data erasure and portability**
  - Provides link to contact Data Controller or to data management platform
  - *(could be extended with link to automatically trigger data erasure or portability; but needs strong identity and identification, Article 29 WP)*
A simple framework

**User interfaces:** collect, stores and manage PDRs and associated Personal Data

**PDR generator:** uses secure APIs from different corporate legacy systems (e.g. Salesforce)

**Audit trail:** authenticity, integrity, confidentiality, non-repudiability
Implementing your PDR

• Step 1 – Identify the target service
• Step 2 – Understand your service
• Step 3 – Make your process ready
• Step 4 – the User channel
• Step 5 – the PDRs generator

Final Recommendation (the PDR Team): multidisciplinary, including UX experts
Use case: smart event registration
Use case: patient data collection

Data Points for PDR:
- Email
- Full Name
- Date of Birth (DoB)
- Phone Number
- Address
- Post Code

Added possibility to manage individual rights

NEW PDR Application

BMS Backend

Booking Confirmation

Response

Data Collected

Visitor

BMS website

PostgreSQL

Hospital/Imaging Centres

Timeframe & Scan Type

Available Slots
Future work

Future work:
- Additional use case: In store data collection – DIY (discussion on going)
- Machine readable format – JSON and LD to standardize categories
- More integration options, using our standard template
- PDRs Trusted infrastructure

How to engage:
- Adopt and integrate PDRs
- Help to develop more implementation friendly tech
Truessec.eu: Understanding consumers

Purpose: create meta-recommendation for labels for security and privacy policies
Covering the following dimensions:
- Legal
- Socio
- Tech
- Business

How: series of panels, involving consumers organizations
https://ktn-uk.co.uk/events/can-you-trust-digital-products-and-services?dm_i=2DZY,14FY7,6ZJSJS,3FLGT,1