cataPULT
Digital

Personal Data Receipts:
How transparency increases
consumer trust

Michele Nati

March 2018

Contents

1. Executive summary

Consumers have trusted so far large internet tech giants to aggregate and use their personal data in return for free services.

EU legislation, through directives such as the Data Protection Directive (1995) and the original ePrivacy Directive (1998), stated that personal data could only be processed lawfully and used legitimately. However, the lack of transparency and the limited user control offered by companies has rapidly undermined consumer trust.

The recently released Mobile Ecosystem Forum (MEF) Consumer Trust Report[1] says that 33% of the new *Savvy Consumers* who were interviewed now demand trustworthy apps and services. Trustworthy apps are those using clear and simple privacy statements that ensure users have full control of their data and trust that it won't end up in the wrong hands.

The online advertising industry has not helped to allay consumer fear in this regard. Examples of this growing distrust of vague, unclear and difficult to read privacy statements, may be attributed to the consumer data leakage caused by *freemium* services. In an attempt to combat this, a growing number of consumers are now adopting advert blockers or even providing false contact details when signing up for these services.

Savvy consumers' demand for trustworthiness and transparency is a key component of the upcoming General Data Protection Regulation (GDPR). Its primary aim is to rebuild consumers' trust by 1) increasing transparency, 2) recognising users desire for more granular control of their data access and sharing, and 3) guaranteeing a set of fundamental individual digital rights (including the right to rectification, erasure, data portability and restricted processing).

This white paper describes the Personal Data Receipt (PDR) work undertaken by Digital Catapult. PDRs provide a tool that can be used to address consumer needs for simple privacy statements and explains how their personal data will be used. Our ambition is to try to reestablish trust in digital services by increasing transparency around the use of consumer data.

Through the paper, Digital Catapult aims to outline the benefits to organisations in developing a standardised Personal Data Receipt process that clearly demonstrates to customers just how their personal data will be used. This paper defines best practices and provides guidance for the creation of PDRs with an objective to initiate an open conversation with companies and organisations that are interested in adopting them via a process of implementation, testing and refinement. We hope that an ecosystem of transparent and compliant user-controlled personal data collection and sharing practices will gain traction in the market.

The objective of this paper is therefore to:

- Describe the importance of transparency in increasing consumer trust when it comes to services that use their personal data.

- Discuss the challenges and opportunities for transparency based on the upcoming GDPR and provide guidance on how PDRs might help organisations to achieve part of this required compliance. Furthermore, to assist SMEs in this market to understand the value of their customers' data and the importance of transparency.

- Illustrate guidelines that will help SMEs to develop and deploy PDRs that leverage Digital Catapult's experience.

- Achieve further engagement with interested technology providers whose desire it is to further develop the PDRs as a set of services that make adoption, integration and deployment easier, more standardised and accessible, even to SMEs with limited resources.

It is hoped that this report will identify a number of opportunities for collaborations aimed at further developing the PDR concept or promote its adoption in the tech community. If you have any ideas that you wish to contribute, email Michele Nati at **michele.nati@digicatapult.org.uk.**

2. The Personal Data Economy:
The opportunity

Trends demonstrate that organisations are currently embracing digital transformation and creating more data-driven businesses through use of customers' personal data. As this practice grows beyond the current predominant social media platforms and target advertising industry, more economic value is expected to be generated in new sectors, including digital manufacturing and digital health. The Department for Digital, Culture, Media and Sport (DCMS) predicts a £241 billion growth in UK revenue[2] between 2015-2020 derived from the use of personal data, with a 11% increase in customer numbers and a 10% growth in new opportunities.

In the digital health sector, Boston Consulting Group (BCG)[3] estimates that the value derived from the use of personal data in Europe, each year, will be around $54 billion and $8B billion respectively for consumers and organisations. Those figures are expected to grow respectively beyond $213 billion and $112 billion by 2020. The potential for this value creation arises from using patient data to create:

1) A holistic approach to healthcare, social care and self-managed well-being.

2) Statistical and deep learning based health decision support tools for doctors.

3) Personalisation of drugs and medical interventions.

Similarly, BCG estimates that the value derived through the use of personal data in the digital manufacturing sector in Europe, each year, will be around $1 billion and $11 billion respectively for consumers and organisations. Those figures are expected to grow respectively beyond $6 billion and $52 billion by 2020. The potential for this value creation arises from using personal data to, amongst other things:

1) Gain consumer insight that leads to better product design.

2) Create connected devices that enable new product functionalities, which are personalised to the user's needs
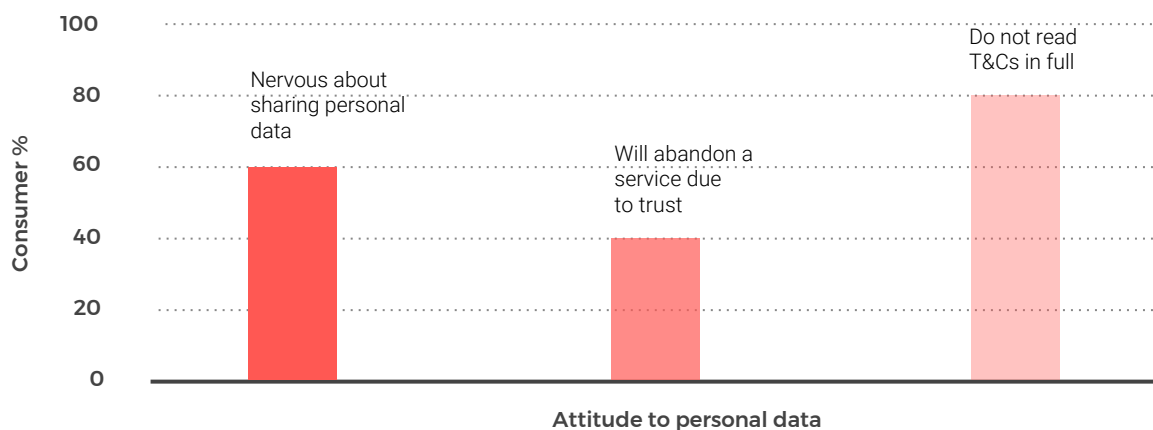
3. The Personal Data Economy:
The risk

Figure 1. Consumer Trends

With the ability to deliver advanced and personalised digital services for their customers, more companies are now also increasing their potential to generate additional revenue streams via the advertising industry.

The lack of transparency and the emergence of savvy consumers is hindering these growth opportunities.

As a result of the growing volume of sales and marketing communications that they are exposed to on a daily basis, more than half of consumers[4] increasingly perceive a lack of control over how their personal data is being used, with 60% feeling nervous about sharing personal data when using digital services. This is due to the lack of transparency regarding how their data is collected and used, as well as the challenges consumers face in tracking and controlling how the data they share is actually used.

Mobile apps users identify trust issues as the primary reason to abandon a service. More often than not, it's because the commonly used privacy policy and Terms and Conditions (T&Cs) statements lack transparency and do not offer a means to retain consumer trust. Whilst only 20% of customers admit to having fully read the T&Cs[5] before agreeing to them, the majority of those customers still demand a new and improved user experience when dealing with agreements of such contracts.

The combination of the above, along with recent data breaches[6], is raising consumer demand for better protection and a clearer understanding of how their personal data is being utilised. The current reaction of consumers regarding the widespread practice of providing false data is resulting in further inefficiencies that undermine the growth envisioned.

To arrest this slide of a growing lack of trust, private and public organisations, including governments, should commit to increased transparency and re-assure customers and citizens that their data is being used in a way that they expect[7]. This practice however requires the advent of new and more trusted customer channels that transparently communicate an organisation's intent.

On the same front, the GDPR, in force in all EU Member States from May 2018 and implemented in the UK through the Data Protection Bill[8], is forcing organisations that currently collect data from European citizens to further investigate opportunities that will increase user trust. This will only be achieved by improving transparency (Articles 12-14 on Information Notice) and allowing consumers more control over their personal data.

The legality of developing these new trusted channels is growing and hence an opportunity to fill this gap is now finally emerging.

4. From Transparency to Trust

Offering transparency on how personal data is used, while increasing the trust of savvy consumers, results in the following benefits for the personal data ecosystem.

For individuals (sharing personal data with an organisation)

Privacy policies will become more human; providing users with a better understanding of what they are letting organisations do with their personal data, without having to read long documents written by lawyers and for lawyers, rather than by actual users of digital services. As a result of increased transparency and control that their personal data will not end up in the wrong hands, user's trust will increase[9]. As a consequence, users will be more willing to share personal information, knowing exactly what it will be used for and how much control they have over their data.

For organisations (providing digital services, collecting and using personal data)

Increasing transparency and building trust with their customers/users requires organisations to clarify how they use and process personal data by providing more simplified privacy statements. By doing that, organisations become an example of a user-centric attitude to personal data and thereby open new communication channels with customers/users, avoid churn, and increase access to quality consumers' data.

5. Transparency and GDPR: Opportunities and challenges

On the one hand, GDPR is requiring organisations, large and small, to perform a greater degree of due diligence when dealing with a customer's personal data, achieved by carefully reviewing their processes and including Privacy and Security by Design principles (and in some case Data Protection Impact Assessments). This is being instituted to avoid large fines handed out due to possible data breaches.

On the other hand, the higher consumer demand for transparency and the granular consent, required by organisations before accessing their data, offers opportunities for those organisations to create new channels and regain consumer trust.

GDPR Article 4 states that consent should be freely given, unambiguous, as well as specific to the purpose, while Article 7 requires a proof of such consent to be maintained by both parties, the *data subject* and the *data controller*.

Transparency and control are at the core of Article 12-14 that requires data controllers (e.g., the organisation deciding the purpose for collecting and using personal data as part of a named service offer) to provide a fair processing *information notice* on how the subject's personal data will be collected and used. This aims to increase transparency over how organisations use the personal data they collect. Similarly, Articles 15-19 demand more user control over their data. Article 15 outlines the *right of access* by the data subject, with Articles 17-19 regulating the rights of the individual, including the *right to be removed from databases* and consequently any personal link to his/her data be removed upon request.

It is clear how a proper implementation of Articles 12-14 will offer the chance to regain trust, provided that the needs of savvy consumers looking for a better user experience are considered and simplification of privacy statements are taken into account. Although recommendations on how to implement specific GDPR articles have started to emerge, it will be hard to satisfy these requirements with a one-size-fits-all solution. As result, there could be additional compliance burdens, in particular for small organisations willing to maintain, regain, or develop customer trust.

This paper intends to present what Digital Catapult believes to be a compliant solution that provides the transparency required by GDPR and the emerging savvy consumers: The Personal Data Receipts (PDRs).

PDRs are a human-readable digital record summarising in a simple and clear way what personal data an organisation is collecting about an individual, for what purpose, how it's stored, for how long and if any third-party sharing is allowed.

For simplicity of implementation and delivery, PDRs can be issued as mobile-friendly email when customers join a new digital service.
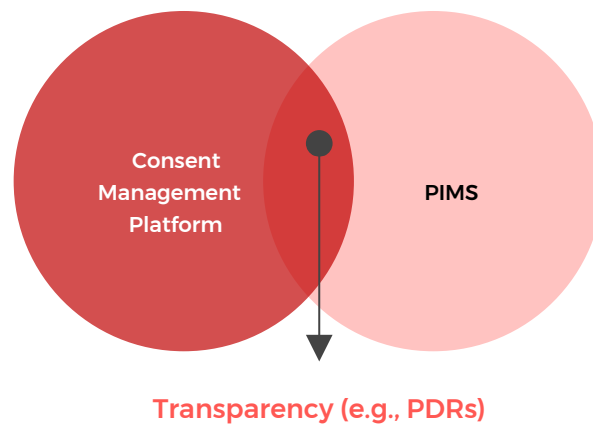
5.1. GDPR compliance: Technology landscape

Figure 1. Personal data technologies landscape

Current solutions for GDPR compliance mainly focus on providing a platform for Consent Management (e.g., mylifedigital[10] and PrivacyCheq[11]) or Personal Information Management Systems (e.g., PIMS, an example of which is digi.me[12]).

Consent Management platforms extend the CRMs of organisations with a dashboard interface that's accessible to end-users and offers fine grained review and access to shared personal data and granular management of consent (mainly through box ticking interfaces). PIMS solutions instead utilise available open APIs to acquire user personal data from existing supported applications and platforms, mainly using OAuth or other authentication standards, and providing access to such data to create new compliant solutions, where the data is used according to user defined policies.

The figure above shows how the current landscape of solutions focuses respectively on compliance to Article 4-7 (Consent Management Platforms) and to Article 15-19 (PIMS), but still without devoting enough attention on the required GDPR transparency and to simply communicate privacy statements to consumers at the time that on-boarding for a new service is

offered.

PDRs do not work as a stand-alone. They could be integrated with services using Consent Management Platforms. PDRs could be issued at the time new customers are on-boarded for given services and could also include a link to the provided Consent Management Platform, the existence of which could otherwise be unknown or difficult for less technical customers to discover[13]. Similarly, new services developed by accessing users PIMS, could issue PDRs for each new service created through user consent and also provide contact details of the new Data Processor who manages the specific service[14] .

6. Personal Data Receipts:
How to increase transparency and trust
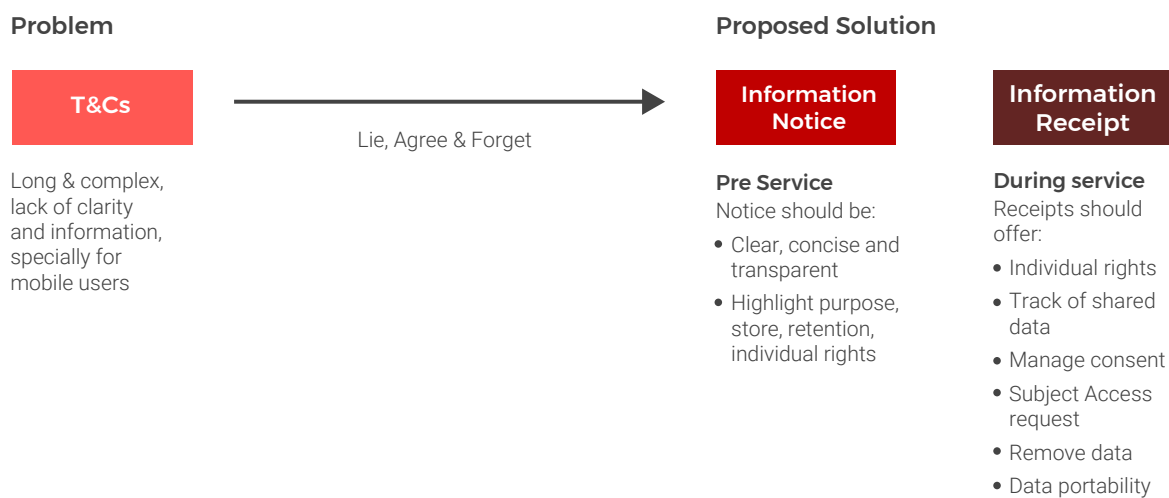
Figure 2. Transparency: Challenges and Opportunities

Terms and Conditions (T&Cs) provide a cumbersome way to onboard savvy consumers to digital services. They now demand far more information. T&Cs are often agreed because they don't offer alternatives, or are seldom read in full or understood. Moreover, they often hinder information on how choices can be altered or a service terminated.

As a result, switched on customers are demanding far simpler and clearer privacy statements that focus more on the user experience, in particular when services are accessed from mobile devices. Failing to provide such transparency, reduces trust and increases the likelihood of customer churn (stats report that 9 in 10 customers are changing a service when they lose trust).

Figure 2 summarises the issues associated with the current T&C s process. Most of the time, consumers lie when agreeing to T&Cs due to the lack of clarity, or simply to access a desired free service. Once this is done, any trace of what has been agreed is lost, making it impossible for consumers to change their decision.

Problem Statement: How to increase consumer trust and business transparency by developing a GDPR compliant solution that takes into account the user experience and helps to reduce consumer pain points? Furthermore, how can this be done without increasing the organisational compliance burden related to the provisioning of digital services using personal data?

To solve this problem, there is a need for a clearer information notice and a way to track choices. To this purpose, Digital Catapult developed, tested and now wish to promote the use of PDRs (https://www.digitalcatapultcentre.org.uk/project/pd-receipt/).

6.1. The design

PDRs represent the current evolution and the practical implementation of user-centric research that Digital Catapult conducted last year. The fundamental research questions we tried to answer were the following: *Does transparency increase consumers trust and how can transparency be achieved and measured?[15]*

The scenario: Almost daily, our physical life intersects with the digital world. To access this world, we are continuously asked to fill in forms and provide personal information. But do we really understand why and do we have any control on what happens next with our personal information? The answer is more than likely NO.

Leveraging a user-centric design, and focusing first on the user-experience, our research showed that providing a clear and concise human-readable receipt (digital record) is an effective method of communicating why personal information is gathered and how it is used when a person signs up for a new digital service. Our hypothesis, confirmed by this initial study and the surveyed participants, was that providing a personal data receipt brings an additional level of transparency in personal data sharing and builds trust between an organisation and its customers.

Despite the amount of details provided by Privacy Policies and T&Cs, the interviewed groups deemed relevant a summary of the following information:

1) The category of personal information the organisation collects to provide a subscribed service.

2) The purpose of collecting the personal information, with particular emphasis on envisioned third-party sharing.

3) The where, how and for how long the personal information is stored.

4) The contact details of the Data Controller to create a way to easily flag the request for removal of shared personal information[16]

Sampled groups welcomed the use of icons, but only if supported by simple, non-technical plain text, which was considered as the main requirement for a meaningful Personal Data Receipt.

The figure overleaf shows the implementation of a PDR, including the categories of information, as per the above bullet points. It has been tailored with the information related to the Privacy Policy applying to visitors of the Digital Catapult Centre in London and registering through our automated concierge system[17].

The PDR was designed with the support of UX and design experts to improve its look and feel, work well on mobile devices, and to properly re-engineer the experience of users when they connect with the Data Controller with the express purpose of executing their digital rights (e.g., data erasure).

Your Personal Data Receipt

The personal information you gave Digital Catapult

- Full name
- Email address
- Organisation
- Signature

The purpose of collecting your personal information

- For your health and safety while you are visiting us.
- For demonstrating to our funders our engagement with organisations.
- If you signed up for it, sending you marketing information.

How your personal information will be treated

Sharing
- If you are a member of the Personal Data & Trust Network we share your details with the Knowledge Transfer Network (KTN).
- Otherwise, we do NOT share your personal information with anyone else.

Storage
- Your personal information is stored securely on servers within the EU.
- We will hold your data for as long as necessary, but no longer than seven years or until you ask for it to be removed.

Information
- If you want us to stop using the above information, for the purposes we've listed, please send us a request and reference the Receipt ID below.

Figure 3. Digital Catapult PDR

6.2. The deployment

Catapult Centre engagement	Weekly Average
Centre Visitors	222
PDRs sent	108
Email open rate	52%
Click through rate	20%

Website engagement	Weekly Average
Visitors	11
Total page views	11
Contact via website	0

DCC visitors (Figures taken cumulative since 13/09/16)	Total receipts sent
Visitors	6158

PDRs sent by interest area	Percentage
Companies focused on privacy & trust	47%
Other areas of Interest	53%

Insights	Yes	NO
Would you like services you signed up for to send you a PDR?	75%	25%
Would you consider implementing something similar within your company?	75%	25%

People interacting with PDR

50%	50%
Opened	**Not Opened**

11% of people who opened the PDR interacted with it

Personal Data Receipts Insights

In order to pioneer the adoption of Personal Data Receipts, the Digital Catapult implemented and issued a PDR to all first-time visitors to its London centre. By doing this, we intend to lead by example and encourage other organisations to adopt a similar approach to increase transparency within customer relationship practices, as well as educate individuals on how their personal data is collected and used.

PDRs are issued daily as part of the automated registration service available to Digital Catapult visitors. We request some personal information in order to complete the registration.

First time visitors signing-in, using our electronic concierge system, are sent a PDR containing details of the personal information they have shared with us and how it's used.

Feedback from visitors is continuously collected to validate our original assumptions, as well as refine and improve the user experience with PDRs. The overall integration process took 4 weeks and was developed in a very agile way, followed by a lean decision process that didn't raise any major issues.

To date we issued over 6,000 PDRs since September 2016. The majority of the recipients (80%) recognised the utility of the PDR as a transparency tool to increase trust in the organisations that issue them. It is worth noting the high rate of PDR recipients that opened the email (50%), indicating the effectiveness of email as the selected communication channel (11% further interacted with the PDR email hyperlinks). To date the number of data erasure requests triggered using PDRs numbered three, indicating that visitors understood and were confident in the way Digital Catapult uses their personal data. We were able to deal with such requests in on average two working days, confirming the effectiveness of the channel created by PDRs to process such requests. However, before the introduction of PDRs, we did only have one such request in three years. This is also a positive sign that PDRs are improving customer understanding of their personal data and empowering them to take action when they are not satisfied about the use of it.
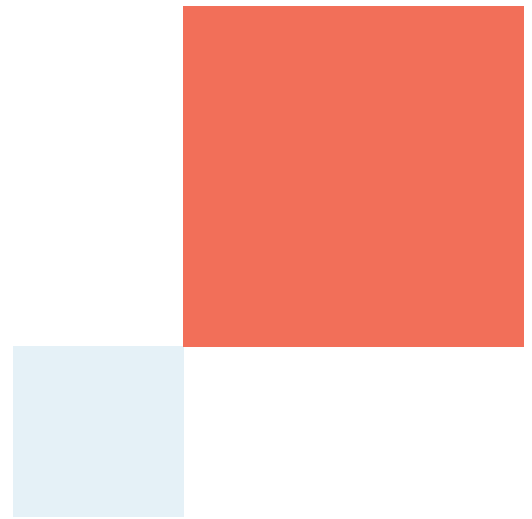
6.3. The implementation
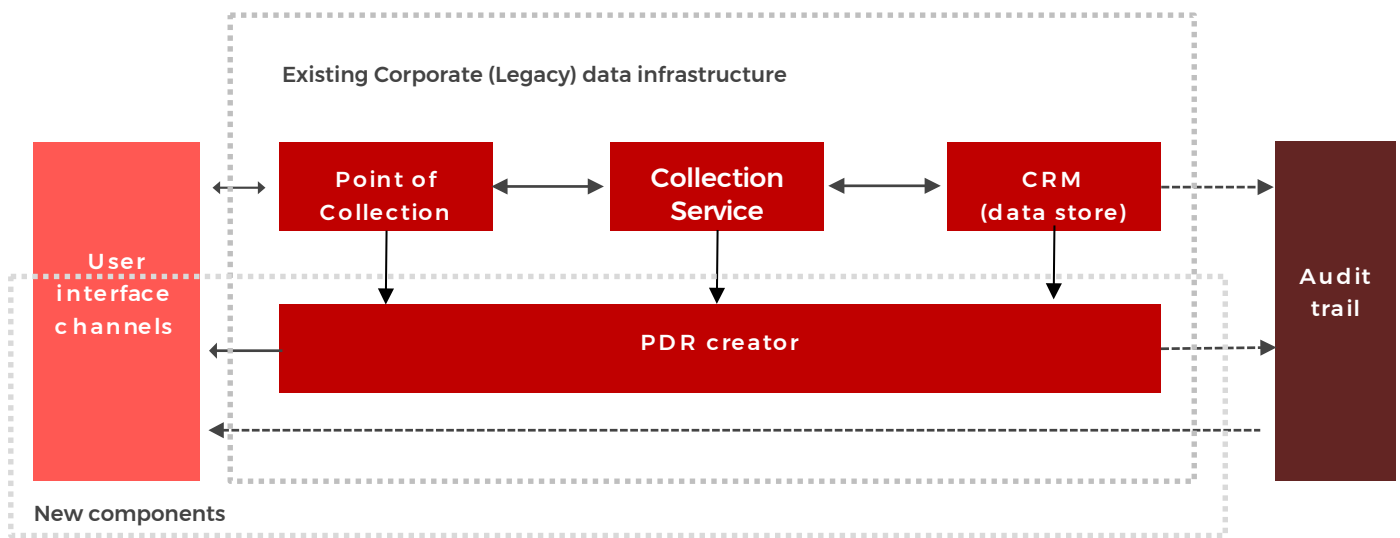
We recognise that many small and medium sized enterprises might lack the availability of technical resources necessary to properly understand the value of customer's personal information and how to manage it with transparency and trust. Digital Catapult's aim is to provide guidelines on how simple it is for smaller organisations to achieve this when using PDRs.

This section provides an overview on how organisations could simply integrate PDRs in personal data management processes and customer relations.

The figure above provides an abstract view of the different subsystem your organisation could employ for personal data collection.

The identified subsystems can be split into existing legacy systems already deployed as part of your service and new systems required for the deployment of PDRs. The existing subsystems include the following:

-**Collection Service** is the backend service that collects (and

needs) personal data from your customers, whether through a mobile app, a web service, etc.

-**Point of Collection** is the interface used to acquire personal data from your customer, e.g., a registration form provided through a web page, or a dedicated personal (e.g., offered through a personal device) or non-personal application (e.g., offered through a shared device, an e-kiosk).

-**Customer Relation Management database** (CRM/data store) is where the collected personal data of your customers are safely stored, processed and accessed.

-**Audit trail** is the separate system already in place that in a personal data related system should at least maintain an access log to the data store.

The new required subsystems are comprised of:

-**User (interface) channel**, is the channel identified for the provisioning of PDRs and the definition of the technology to be used to deliver the PDR. This can include emailing clients (and

emails), e-wallet (and e-wallet pass), dedicated (existing) mobile apps or web dashboards (and notification and document, e.g., pdf-based PDRs, store).

-**Personal Data Receipts (PDRs) Creator** is the new component (or combination of components) that creates a personalised PDR, delivered using the selected User Interface and maintains a compliant audit trail of the overall process (e.g. 'versioning' of the relevant privacy policy).

Because savvy consumers demand better user experiences when it comes to deciding whether to share their personal data, the implementation and integration of PDRs requires multi-disciplinary expertise. This will also facilitate a successful and smooth integration process.

Recommendation (The PDR team): To create a meaningful PDR for your digital service, you will need the following in order to assemble a small multi-disciplinary team in your organisation: a UX expert to simplify the user interaction; a lawyer to ensure you are not misinterpreting the law by simplifying the communication, a technologist to ensure security, privacy and compliance.

Assuming you have created a team for the implementation of PDRs in your organisation, the following steps are required in order to deploy your Personal Data Receipt:

Step 1 (Identify the target service): The first step when issuing a PDR is to identify the provided digital service (e.g., the Collection Service that collects your customer's personal data) of which you want to enhance the transparency and control with the integration of PDRs.

Step 2 (Understand your service): The second step is to understand the user journey undertaken to subscribe to the given service, identify the associated Privacy Policy and the Terms and Conditions, discover the associated personal data flow within your organisation (e.g. perform a GDPR required Data Privacy Impact Assessment) and identify the relevant subsystems that forms part of it (the Point of Collection, the Customer Relation Management data store and the Audit Trail). Use the chance offered here to understand if all the personal data you collect is required and if not desired, how to minimise it.

Step 3 (Make your process ready): The third step before integrating and rolling out PDRs, is to understand and adapt your

process to deal with subsequent requests (e.g., data erasure) from your customers. It's a GDPR requirement to provide customers with the ability to execute their individual digital rights, so your system and business processes need to be ready for that.

Step 4 (The User channel): The fourth step is to select the user channel used to deliver PDRs and receive related requests triggered by your customers. If no other channels are in place, emails might represent the easiest way to initially build such a channel. However, consider that emails might sometimes not always be an effective channel to grab user attention (e.g., pay particular attention to how you choose the subject of your PDRs email) and that those emails might require more effort to protect the security and privacy of issued PDRs.

If you select emails as a User channel, you can always re-use and expand our PDR template. Our template can be downloaded, customised and used for your services under Creative Common Attribution 4.0 International License (free to share, free to adapt).

Step 5 (The PDR Creator): The last step is to implement the PDR creator and to maintain a consistent audit trail of the issued PDRs. The information required by the PDR creator can be provided by any of the Collection Service, Point of Collection, or Customer Relation Management database and shared through implementation of secure APIs.

If you decide to implement your PDR creator with information received from your customer database and to deliver PDRs using email, always implement best practices for secure communication (e.g. HTTPS) between different subsystems.

More details on the technical integration of PDRs within the Digital Catapult system and a blueprint architecture with guidelines for integration with other systems are available on request.
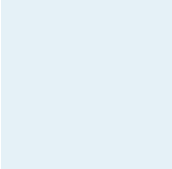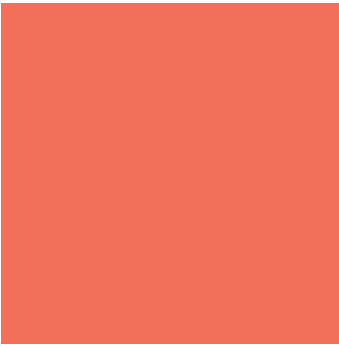
6.4. PDRs and GDPR

In this section, we highlight the relevant GDPR articles and discuss how PDRs are a tool used to address the requirements of transparency and user control.

Because PDRs are issued when a user joins a new digital service, by expanding the categories of collected data with information on those collected under consent, compliance to Article 7 (Proof of Consent) is guaranteed. However, in this case, PDRs become a tool integrated by a Consent Management platform. Our intention was instead to increase transparency and eventually simplify management of individual digital rights. The following table provides an explanation on how this is achieved.

Article	What PDRs Offer
(12-14) Right to be informed	PDRs provide a standardised human-readable template designed by consumers for consumers. They allow data controllers to easily customise and deliver all the information required by the 'right to be informed'. Moreover, instead of showing this information on generic web-pages, they deliver it through personalised digital means (e.g. emails) and embedding data controller contact details. This opens up a direct channel between data subject and data controller. Using a unique ID simplifies the linkage of additional personal data to a specific data subject and opens the door to automatically update and notify the customers of the future acquisition of their additional personal data (e.g., after a Privacy Policy is revised).
(15) Right of access	PDRs generated for any existing or new personal data transaction (e.g., acquisition of personal data by a data controller from a given data subject in relation to a provided digital service) will automatically link a data subject to any related personal data already stored in a data controller system using a unique pseudonymous ID. In addition, PDRs provide a direct and convenient channel to automatically trigger an access request from a data subject.
(16) Right to rectification	Through the requirement to list third party sharing, PDRs create good practice for linking data subject information to specific third parties receiving them, thus simplifying cascade updates. Moreover, PDRs can make data subjects responsible for identifying given data categories that require rectification as well as providing a channel for such updates. This will not require anymore previous subject access requests to first discover collected data. This can turn into an overall saving in managing such and similar user rights. Updated receipts can be issued at any time that a new third-party sharing is consented for the same set of personal data.
(17) Right to erasure	PDRs provide a direct channel that links data subjects and their personal data with data controllers, thus simplifying the notification and management of the right to removal. Being issued as a copy to the data subject, PDRs also promote best practice for data subjects to review their personal data sharing. This allows them to track different ongoing personal data sharing activities and easily identify those not currently being required anymore and subject to request for removal.
(18) Right to restrict processing	PDRs provide a direct channel that links data subjects and their personal data with data controllers, thus simplifying the notification and management of the right to restrict processing, while educating customers on how their data is being used for automated decisions.

Article	What PDRs Offer
(18) Right to data portability	PDRs provide a direct channel that links data subjects and their personal data with data controllers, thus simplifying the notification and management of the right to portability. By automatically linking relevant personal data to specific data subject initiated requests, PDRs avoid inefficiency associated to discovery of data affected by specific requests.
(21) Right to object	PDRs provide a direct channel that links data subjects and their personal data with data controllers, thus simplifying the notification and management of the right to object. By embedding information related to the purpose of processing PDRs, it provides grounds for data subjects to understand the right to object.

The list is not supposed to be exhaustive, but it should already provide evidence of the utility and further benefits and advantages derived from adopting and extending the Personal Data Receipts. It should motivate for best practice in creating transparency and trust for personal data sharing. It is clear how PDRs in their current form already provide a new channel that addresses savvy customer needs to swiftly manage GDPR requirements for transparency and for data subject rights management.
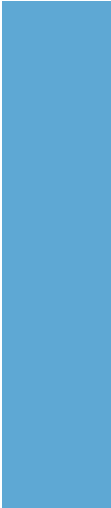
7. How to get involved

There are a number of use cases and scenarios in which PDRs can help to increase transparency on how personal information is used, and can help organisations to increase customer trust. In particular, based on the feedback we collected, it is clear how the additional transparency provided by PDRs helps to expand the services delivered by either unknown or already trusted brands. This also confirms what savvy customers require in order to trust the myriad of services they are exposed to throughout their digital experience.

As in our proof of concept demonstration, PDRs work particularly well in situations where collection of personal information occurs in real-life events that usually initiate new digital services, such as in-store purchases, loyalty programmes onboarding, telephone taxi bookings and patient-doctor relations. In such scenarios though, customers have little opportunity to distill and check how their personal information is being used and how to exercise control over them.

In addition, we identify a number of systems and channels that could be used to integrate and issue PDRs. A number of tools and APIs can be developed to provide integration with an external PDR creator. Providing such seamless integration will promote the widespread use of PDRs.

We are therefore now looking for a combination of both. New adopters of PDRs (in particular large organisations that might pave the way for their diffusion) and technology providers (in particular SMEs) that want to help us extend the current concept into a more viable technical solution.

We have so far organised three engagement workshops during which we presented the Personal Data Receipts concept and our Digital Catapult implementation. We then asked participants to identify and co-design use case scenarios where PDRs could help, based on experience and services their organisations are providing.

As results of these workshops, we implemented PDRs in three more scenarios, and are currently discussing more partnership

opportunities that emerged from this initial engagement.

We hope that this report will help you to identify other ways to get involved and collaborate with us in making the overall personal data ecosystem more transparent and trusted.

If you want to get involved, we want to hear more about your ideas by emailing michele.nati@digicatapult.org.uk

8. Acknowledgements

This project was inspired by the future need for compliance with GDPR; guidance by the ICO on layered privacy notices; the guidelines on information notice from Article 29 WP and the Consent Receipt standard under development within the Kantara Initiative and its Consumer and Information Sharing Working Group (CISWG), an industry-led consortium focused on identity services.

A special thank you goes to our Summer 2016 PhD Intern Tatiana Styliari, who first conducted testing on the viability of the Personal Data Receipt concept. In addition, thanks must go out to the Digital Catapult team that contributed to the implementation of a first Personal Data Receipt: David Ponsford (Product Manager), Hua Xang (UX tech lead), Stephan Garcia (Sales Force Manager), Tessa Conway (Senior SW Engineer), Richard French (Legal Director) and Lucie Burgess (Head of Personal Data and Trust Programme).

9. References

[1]Global Consumer Trust Report 2017. https://mobileecosystemforum.com/programmes/consumer-trust/global-consumer-trust-survey-2017/

[2]Unlocking the power of data in the UK economy and improving public confidence in its use. https://www.gov.uk/government/publications/uk-digital-strategy/7-data-unlocking-the-power-of-data-in-the-uk-economy-and-improving-public-confidence-in-its-use

[3]The Value of our Digital Identity. Boston Consulting Group. https://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

[4]Data Protection Eurobarometer report. http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

[5]The average length of T&Cs which was 2000 words in 2012, with an average reading time of 10 minutes is constantly growing

[6]https://www.theguardian.com/business/2017/aug/10/talktalk-fined-100000-for-not-protecting-customers-personal-data

[7]UK Government Transformation Strategy 2017-2020: https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy#make-better-use-of-data

[8]UK Data Protection Bill, September 13th: https://www.gov.uk/government/collections/data-protection-bill-2017

[9]Interviewed users sample confirmed this: https://www.digitalcatapultcentre.org.uk/project/pd-receipt

[10] https://www.mylifedigital.co.uk

[11] http://www.privacycheq.com

[12] https://www.digi.me

[13]Current implementation of PDRs is not meant for consent management although similar extension can be envisioned

[14]By creating a personal data marketplace, PIMS enabled services and apps are usually developed by third parties that discover and access user data accessible through PIMS

[15]Research performed by PhD intern Tatiana Styliari, University of Nottingham https://pdtn.org/wp-content/uploads/Researching-the-transparency-of-PD-sharing.pdf

[16]It's interesting to notice how this was requested already before GDPR increased attention

[17]Envoy: The new standard for visitor registration. https://envoy.com

CATAPULT
Digital

We work with
Innovate UK