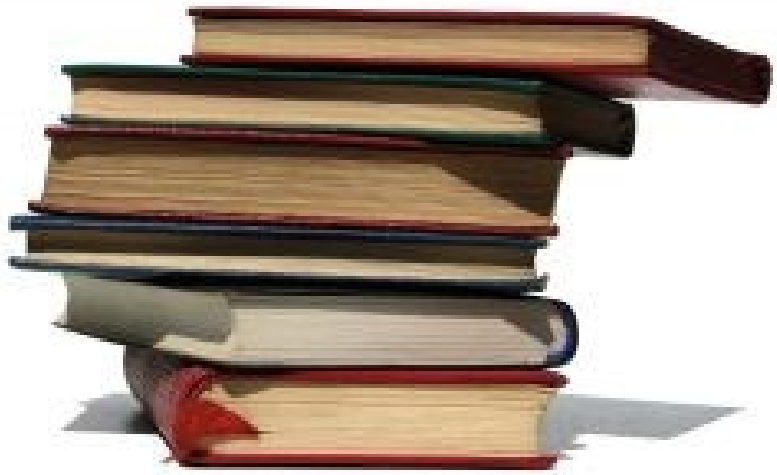
ANEC POCKET GUIDE

Using Consumer Data

Data transfer, trading and privacy



Raising standards for consumers

Disclaimer: this pocket guide is intended for ANEC membership and ANEC representatives in particular.

Summary

This ANEC and BSI/CPIN document outlines personal data sharing by organisations through data transfer and trading practices and the wide spread use of consumer and citizen data. It then examines the issues raised for consumers and citizens by such widespread use of their data when it is spread across so many parties. Then guidance is provided on key technical requirements to address such issues.

1. What do we mean by personal data transfer and trading?

After an organisation has collected data from us, for a purpose that we have agreed to or is legally allowed, it is not unusual for the data to be passed on or disclosed to others either within an organisation or between organisations. This happens in a number of ways as illustrated in the bullet points below:

- a reciprocal exchange of data;
- one or more organisations providing data to a third party or parties;
- several organisations pooling information and making it available to each other;
- several organisations pooling information and making it available to a third party or parties;
- exceptional, one-off disclosures of data in unexpected or emergency situations;
- different parts of the same organisation making data available to each other;
- trading of data sets between parties

2. The scale of personal data transfer and trading

The use of personal data well beyond the initial collection organisation is widespread.

To quote http://www.dataprotectioneu.eu/ "***The automatic processing of personal data is growing at an incredible pace and is starting to become an integral part of economic, administrative and social processes in Europe and throughout the world***."

Note: this statement is given on behalf of over 100 leading European Academics taking a position since February 2013 and published in the German paper "Die Zeit"

Further a very informative paper[1] has been produced by the USA Federal Trade Commission, May 2014 giving a US consumer perspective on large scale data sharing practices represented by "data brokers". This report found that:

- Data Brokers Collect Consumer Data from Numerous Sources, Largely Without Consumers' Knowledge
- The Data Broker Industry is Complex, with Multiple Layers of Data Brokers Providing Data to Each Other
- Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer
- Data Brokers Combine and Analyze Data About Consumers to Make Inferences About Them, Including Potentially Sensitive Inferences
- Data Brokers Combine Online and Offline Data to Market to Consumers Online
- Consumers Benefit from Many of the Purposes for Which Data Brokers Collect and Use Data
- At the Same Time, Many of the Purposes for Which Data Brokers Collect and Use Data Pose Risks to Consumers
- To the Extent Data Brokers Offer Consumers Choices About Their Data, the Choices are Largely Invisible and Incomplete

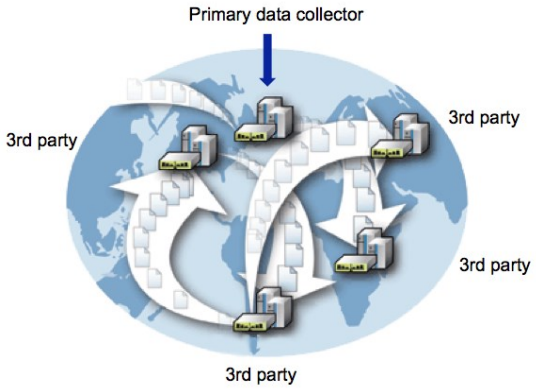
There are other key non-commercial areas of data transfer and trading too. For example in the not too distant future we can expect

[1] *http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf*

that smart cities will extend personal data transfer and trading between many parties in order to improve public services, support innovation and economic growth, and that health services will increase the transfer and trade of personal data for similar reasons and so on.

3. Objective of the guidance paper

Transfer and trading personal data is now widespread and so the aim of this paper is to identify good practice that consumer representatives can propose through their participation in technical committees dealing with such issues, for example in Health and Social Services, Children's interests, Smart Cities, Financial Services as well as traditional Information and Communication Technology (ICT) standards committees.



The manner in which so many markets and services already operate means that improvement from the consumer perspective will not be rapid. Instead the spread of good practice could be expected to be slow at first. This issue is examined in section 13 for an explanation of how the requirements in this guidance, if taken up, might reasonably be used to spread more good practice.

4. What are the consumer issues raised by data transfer and trading practices?

Widespread personal data transfer brings with it issues of:

- subsequent consent to processing by the 3rd parties who receive that data,
- withdrawing consent to processing by 3rd parties after an initial consent has been given or used

- how to deal with personal data access requests when data has been passed to 3rd parties,
- how to ensure personal data is corrected when the records to be corrected have been copied to many different parties,
- dealing with the right to be forgotten when the personal data to be forgotten is held by many different parties
- limiting the use of children's and young persons' data

5. Subsequent consent to use of personal data by 3rd parties.

A useful scene is set by the UK Information Commissioner's Office (ICO)

http://ico.org.uk/for_organisations/data_protection/the_guide/principle_1

Box 1 UK ICO Guidance to organisations - data sharing consent

"Is it ever acceptable to disclose personal data to other organisations for them to use for their own purposes?

It depends. You may be approached by a third party seeking personal data about one of your employees or customers. For example, the police may want information in connection with an investigation, or an individual may want information to pursue legal action. In such cases, you may choose to disclose the information if the conditions of a relevant exemption are satisfied.

Unless one of these specific exemptions applies, individuals should generally be able to choose whether or not their personal data is disclosed to another organisation. If your intention to disclose information in this way was not made absolutely clear at the outset, at a time when the individual had the option not to proceed in their business relationship with you, then you will usually have to get the individual's consent before making such disclosures.

A decision to share personal data with another organisation does not take away your duty to treat individuals fairly. So before sharing personal data, you should consider carefully what the recipient will do with it, and what the effect on individuals is likely to be. It is good practice to obtain an assurance about this, for example in the form of a written contract."

In box 1 the section shown in italics is, unfortunately, generally not true for consent to transfer or trading with specific named organisations and in many cases the situation is such that the primary personal data collector has embedded consent to data transfer or trading into access to their goods or services i.e. you can't buy the product or use the service unless you do consent to the sharing of your data with unnamed 3rd parties.

6. Personal data access requests

When considering personal data access then guidance from the UK Information Commissioner's Office (ICO) and other European data protection authorities is that there are a number of personal data access request rights - see Box 2. These rights are made much more difficult or impossible to exercise given current data transfer practices.

Box 2 *UK ICO Guidance to organisations – right of access by an individual to their own data*

In brief – what is an individual entitled to?

This right, commonly referred to as subject access, is created by section 7 of the Data Protection Act. It is most often used by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed,
- whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/access_to_personal_data

There is for example a 60 page UK Code of Practice related to this aspect of Data Protection and Privacy which may be found at:

http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

While box 2 and the UK Code of Practice describes the right of access to the prime data collector it does not address the consumer issue of finding out what data 3rd parties have when the individual's data has been passed on to, and in many cases aggregated by, 3rd parties into a much fuller set of data about each individual. So for an individual to find out just how much personal data aggregators and data brokers hold about them is very poorly supported in practice.

7. Personal data correction

Once an individual has accessed their own data they have the right to get incorrect data corrected. This is illustrated in Box 3.

Box 3 - UK ICO with respect to personal data correction

"The fourth data protection principle requires personal data to be accurate. Where it is inaccurate, the individual concerned has a right to apply to the court for an order to rectify, block, erase or destroy the inaccurate information. In addition, where an individual has suffered damage in circumstances that would result in compensation being awarded and there is a substantial risk of another breach, then the court may make a similar order in respect of the personal data in question."

http://ico.org.uk/for_organisations/data_protection/the_guide/principle_6/correcting_inaccurate_personal_data

Just as current data transfer practices make access to personal data records spread across many parties difficult / impossible then so too these same current data transfer practices make the correction of that data across so many different 3rd parties difficult or impossible.

8. The right to be forgotten

The right to be forgotten is underpinned by existing Data Protection legislation and it is within the proposed revision to EU Data Protection law – see Box 4.

To date it is proposed by the Commission to make the right to be forgotten more effective for individuals, by proposing reversing the burden of proof: it is for the company – and not the individual – to prove that the data cannot be deleted because it is still needed or is still relevant.

Ref: *http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf*

The governance requirement with respect to such determination by an organisation on whether personal data should or should not be forgotten is addressed in the ANEC / BSI/CPIN guide on the Use of Consumer Data.

Box 4. Current Data Protection law underpinning the right to be forgotten.

The Data Protection Directive: Article 12: Right of access

Member States shall guarantee every data subject the right to obtain from the controller: (...)

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Ref: *http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf*

As in sections 6 and 7 the right to be forgotten involves access to your own data and correcting it where, with current data transfer practice, this is difficult/impossible. So it is possible on many occasions for organisations to argue that Box 4 item (c) applies i.e that the involvement of 3rd parties in correcting or forgetting personal data is "impossible or involves a disproportionate effort".

9. Especially important data sharing contexts

There are some special cases where improving current data transfer practices, as outlined in sections 10, 11 and 12, may be especially useful in underpinning the law and public interest in specific cases

where poor data transfer practice currently severely hamper them. Such special data transfer or trading areas include

- Limiting the use of children and young persons data by 3rd parties
- Dealing with money laundering and financial fraud
- Ensuring privacy of individuals' most sensitive personal data

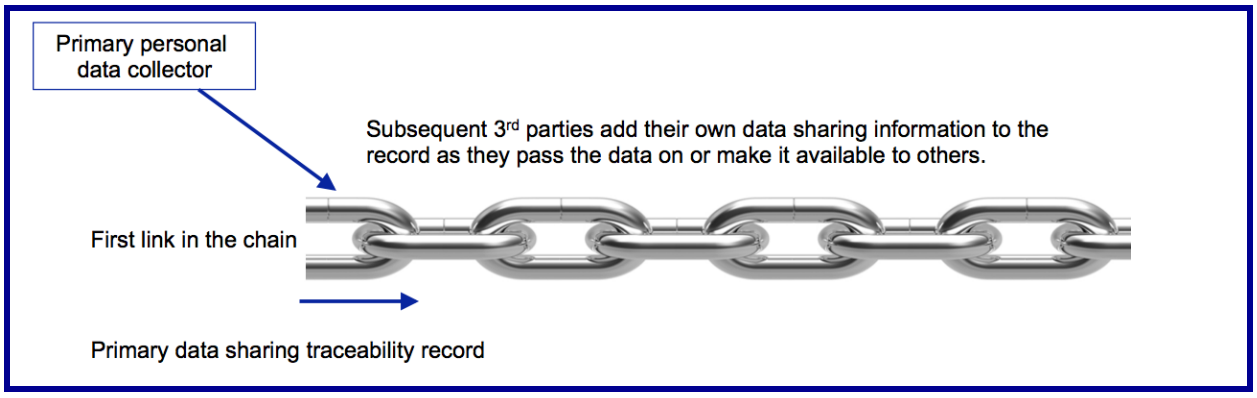
10. Data transfer and trading transparency i.e. "Who has my data?"

10.1 Data transfer traceability - technical requirements

When personal data is passed to and processed by third parties other than the original data collector, then being able to find out who has your data and what of your data they have is essential. So traceability is required to enable 3rd parties to be found for personal data access, correction, right to be forgotten and ensuring good practice consent management.

The first step has to lie with those who first collect personal data and then transfer it with others. In figure 1 the primary data collector would create the initial traceability record, which others would then have to add to in order to maintain the chain of traceability.

Figure 1 – First link in the data sharing chain



The requirements for data transfer traceability records should include:

i. A record of who the primary collector was and the consent given to what processing purposes
ii. When the data was collected
iii. Records of anonymity steps, if any, taken pre data sharing

iv. What data types/fields have been passed on or shared
v. Records of which organisation or person passed personal data to whom by whom and when
vi. Records that deal with sharing of single individual's data or the sharing of data sets covering more than one individual
vii. Traceability records that are structured to allow forward and backward path tracing

This data sharing traceability capability underpins the issues raised in sections 4-9.

10.2 Other necessary data transfer records

It should be noted that transparency of personal data transfer records also need to meet the requirements of personal data analysis when shared data is used. These are given in the ANEC / BSI CPIN guide on the Use of Consumer data. These additional requirements arise at least in part from the need to assure the fitness of data for analysis purposes and the accuracy of subsequent results from such data analysis of transferred data.

These additional data transfer requirements for personal data analysis are:

The shared personal data set records should include

- what the data set includes
- why it was collected
- who was responsible for the collection,
- data collection methodologies,
- analysis methods used for derived data in the sets,
- any personally identifiable information collected
- privacy risks and controls

A good example of this approach is the "USAID Open Data Privacy Analysis Template."

A Mandatory Reference for ADS Chapter 508

New Reference: 03/07/2013

Responsible Office: M/CIO/IA

File Name: 508mah_030714

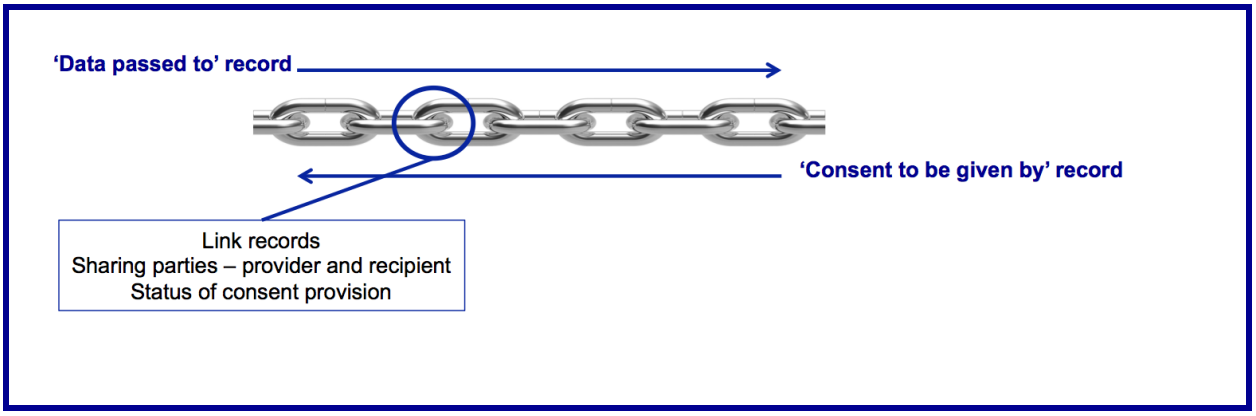
11. Consent Traceability – technical requirements

11.1 Consent traceability to new processing purposes

When personal data has been transferred to others then basic good practice includes gaining consent to any new processing purposes undertaken by a third party.

The traceability requirement given in section 10.1 vii, dealing with forward and backward traceability to be achievable from traceability records, is essential to enable this need for consent provision to be met.

Figure 2 – Tracing back to individuals in order to obtain consent



Where 3rd parties do not have direct contact information for an individual then this backwards traceability allows those 3rd parties to find the primary data collector and enable contact to be established with the individual(s) involved.

It should be noted that, ideally, the detailed standards requirements established to realise this good practice should support automation of the process to minimise costs and administration burdens.

11.2 Consent traceability within original data processing consents given

It is also good practice to gain consent to processing by a third party when the processing purpose is the same as consented to in the original collection by the primary data collector.

Two examples from the consumer perspective of the need for consumer choice in the subsequent consent following data transfer for purposes already agreed to would be:

- where the individual considers the 3rd party to whom the data has been transferred to be unethical or to have given them poor service in the past, and as such the consumer would not have given consent to the processing purposes if the 3rd party had been the original primary collector.

- where a 3rd party is using the transferred personal data consent to a processing purpose provided by the consumer to the primary collector and that original consent was not optional in order to obtain a good or service i.e. consent had to be given to obtain the good or service. Then enabling subsequent consent to similar processing by a 3rd party is good practice as this consent decision is not subject to those constraints on consumer choice thereby allowing greater discretion and choice by the consumer with respect to that 3rd party processing.

11.3. "Where did you get my personal data from?"

There are a number of situations where a consumer or citizen may be approach by a 3rd party unexpectedly and the individual concerned will choose to ask where this 3rd party obtained the personal data that:

- meant the individual was a 'target' for the initiated communication

- enabled the 3rd party to obtain contact details like telephone numbers and e mail addresses

Good practice in such a situation should require that the 3rd party may, in order to satisfy the individual's request, be allowed to initiate a data sharing transparency request on their behalf.

12. Managing Data Sharing Traceability Requests

12.1 Valid traceability of data sharing requests "Are you who you say you are?"

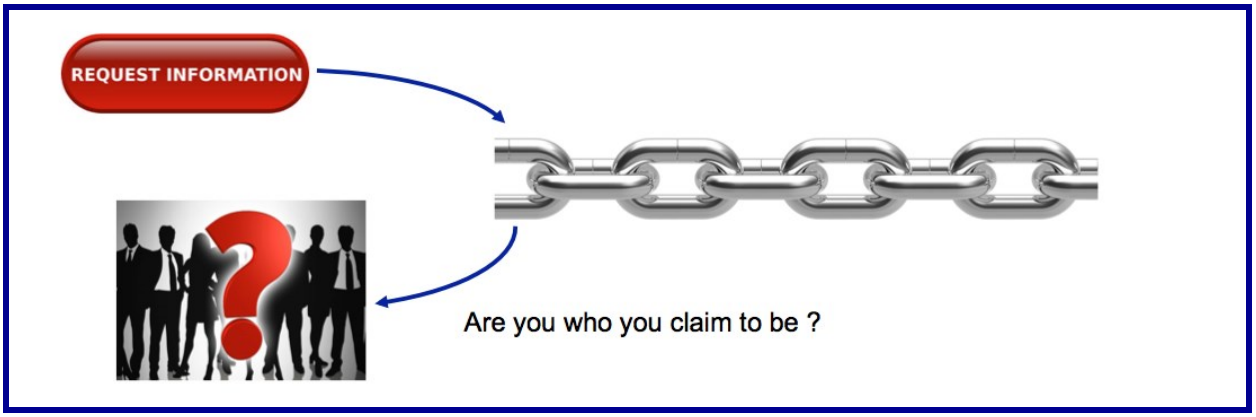
The requirements outlined in section 10 give individuals the practical ability to ask primary data collectors which organisations the

primary collector has transferred their personal data to. When a request for that information is made then basic privacy requirements dictate that only the individual concerned should be allowed access to the answer to such a request.

So data transfer traceability requirements will also need to include validation of requests whether from the individual concerned, from an authorised agent of the individual concerned or from a body with the necessary legislative backing to request such traces.

However, verification of the individual's identity should be reasonable. In any case, a controller should not retain personal data for the unique purpose of being able to react to potential requests (Recital 52 of the proposed European Union Data Protection Regulation).

Figure 3 – Validating data sharing traceability requests



13. Spreading good practice - Finding illegal use and poor broking practitioners

The aim of the standards guidance provided in this paper is to enable the impact of good practice based on these standards to help regulators, law enforcement, consumers and citizens to identify more easily where good practice is not in place and through that take appropriate action.

The key concept is that good practice primary data collectors implement data transfer traceability thereby allowing those further down the chain who "break the chain" to be identified.

Figure 4 - Breaking the chain – identifying the party concerned

The data sharing records of good practice organisations show who data has been passed to and if the receiving organisation breaks the chain they can be identified by records at the preceding "link"

If a data transfer traceability chain has been broken then the traceability records that are complete will take the trace up to the doorstep of the organisation that has not then fulfilled the good practice data sharing traceability standards. That then enables any appropriate action to be taken by the consumer and/or the authorities.

ANEC in Brief

ANEC is the European consumer voice in standardisation, representing and defending consumer interests in the development of technical standards, in the application of conformity assessment schemes to standards, and in the creation or revision of legislation on products and services. ANEC receives funding from the European Commission and the EFTA Secretariat.

ANEC, the European Association for the Co-ordination of Consumer Representation in Standardisation

Avenue de Tervueren 32, box 27 – 1040 Brussels – +32 (0)2 743 24 70
anec@anec.eu - www.anec.eu

http://twitter.com/#!/anectweet

http://companies.to/anec