Comments on Article 29 Working Party Guidance on Data Portability – Boots UK – 31st January 2017.

Context:

Boots is a large multi-national retailer. We operate a customer loyalty scheme (expunged). In order to administer the scheme we hold PII in regards to these customers which is utilised in a number of ways, outlined in our privacy policy.

Transactional data is held separately to PII, however is pseudonimised rather than anonymised and so can be linked to PII through a unique identifier and, as such, would be subject to these guidelines.

(Expunged)

Impact on Loyalty Card Schemes

Our Loyalty scheme is widely considered one of the most generous in the market and is at the heart of our business proposition. We can maintain such a generous scheme because, in return for the rewards we offer our customers, they provide us (with appropriate consents) with rich data through using their Loyalty cards. This data allows us to better understand our customers and develop our business in a way that both benefits our customers and allows us a competitive advantage. Depending on the speed with which our competitors move to take advantage of the new portability requirement, we (and retailers with similar loyalty schemes) may find our schemes being undermined. We reward customers for sharing their data with us but portability will effectively dilute that exclusivity by allowing our competitors legitimate access to this data, at the request of our mutual customers.

This will also involve significant cost to us, incurred either through the need to employ members of staff to furnish these requests, or through IT developments and security measures required in automating them. (Expunged)

While we appreciate that data portability does introduce some potential benefits to business, it is likely that the benefit will, in the short term at least, be skewed towards companies which are already heavily tech-oriented (for example, Amazon) and therefore better placed than traditional retailers to move fast to absorb the newly-available data and utilise it to their advantage. For more traditional bricks and mortar companies, especially those with multiple data sources such as ourselves, this type of development is likely to take longer. We are concerned, therefore, that high street retailers may be more heavily impacted than online retailers.

Continuing Customer Relationship

From the original GDPR legislation we had believed that data would be ported if a customer decided to end a contract – similar to porting between banks currently. There are circumstances within the healthcare divisions of our own business where this would seem logical, e.g. if a customer chose to move their custom between opticians, or pharmacies. However, as portability is now confirmed as not triggering deletion/account closure, but is to be an ongoing right within a continuing business relationship, this is likely to be considerably more time and resource intensive and will certainly prove difficult to deliver within the timeframe required for the GDPR.

Data Protection v Data Access

Whilst we appreciate the value of customer choice and support the need for customers to have clear and accessible rights in respect of their personal data, providing a customer with ongoing access to all of the applicable data is not a small task to undertake. Much of the data we hold would make no sense to the customer or to another business in the format in which it is held and to make it useful to either recipient would require us to invest considerable work in 'translating' it. As our customers might be 'porting' their data to retailers, loyalty scheme providers or healthcare providers, all of which might use different language and terminology, it will be difficult to ensure that the data we provide (or potentially receive) is understandable and therefore capable of being used. In addition, as there is potential to port data across European borders, this could lead to additional complications. We note that the guidance states that data should be provided in a commonly used format, but it does not address the issue of common language and terminology. We believe that clear guidance and common standards will be essential if portability is to be workable and valuable, and that this must be initiated at European, or at least individual Member State level in order to have the necessary momentum.

In terms of the use of APIs, we consider that the intent is good, as it would give more ready access to data relating to a particular customer, but that it also introduces risk in terms of data security. It is therefore risky to suggest companies move swiftly towards this type of solution, as it needs to be thought through in detail to ensure data is available yet still secure. For example, how could we be sure that a competitor has a customer's consent to request their information? How can we ensure we have an appropriately secure method that will work for all of the theoretically vast range of competitors from which a portability request could originate? How would we ensure that the data provided was accessible to the recipient, without encouraging a customer to give the new company any of the security details unique to their use of our service?

Commonly Used Format

The format for interoperability needs to be defined further, otherwise there is a risk that businesses will diverge in their efforts causing issues further down the line. While customers will be able to request their data, the resulting format may not be readable by the ingesting company. We are concerned that, in the UK at least, there is so far no clear appetite on the part of businesses in our sector or of relevant industry bodies to move towards facilitating data portability and it seems unlikely that interoperability standards will be agreed before May 2018 as this will require significant coordination across sectors and, potentially borders.

Even if all organisations were to chance upon the same file format, there are risks that data could be misinterpreted by ingesting systems as field definitions will not be consistent across different businesses. This could reduce the value of portability or even result in serious harm. An extreme example of this in the healthcare sector may be where over the counter medication bought by a customer in the UK is shared with a company in Ireland. If the product has a similar name but a different formulation in each country, these could be picked up as the same product in error potentially putting the customer at risk and also resulting in some liability for the sending or receiving company.

Audit history

Along with the information ingested, we are unclear as to whether there is a requirement to be able to attribute that information to the originating business in case the customer questions the accuracy or origin of the data in the future? We would like to see clear guidance on the audit requirements around ported data to reduce potential confusion and inconsistency.

Summary

We understand the motivation behind the right of data portability, and can see potential benefits for the customer and for business. However, we also believe there is potential for detriment to both if portability is not implemented consistently and with sufficient forward planning. We believe the benefits can only be realised, and the detriment avoided, through consistency, security and clarity of purpose and operation. We do not believe this can be adequately addressed by individual businesses or sectors and would therefore support the issue of more detailed, practical guidance by WP29 and/or the Data Protection Authorities in individual member states.