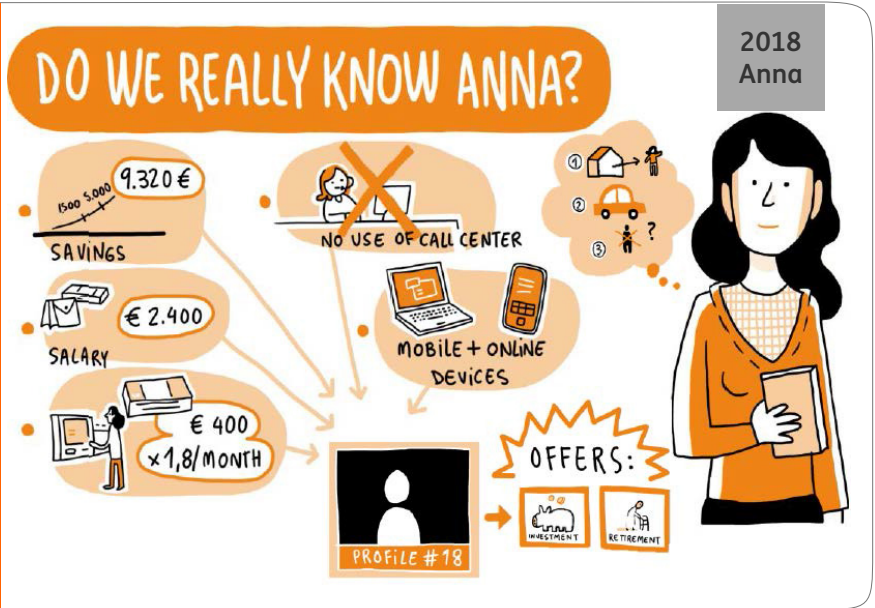


Ensuring a coherent framework for access to customer data



“Our customers expect us to make banking more digital, more innovative and more client-oriented. Meeting these expectations is our top priority.

Given the ever-growing relevance of data in today’s society, I believe customer data should be accessible in a similar manner for banks and non-banks. This should be adequately reflected in the EU’s regulatory framework.

Innovation can certainly flourish within the boundaries of a strong personal data protection framework through which we will safeguard people’s fundamental right to privacy in the growing data economy.”

Ralph Hamers
CEO ING Group



A fundamental shift in customer expectations means the European economy is increasingly driven by data-created value. The regulatory framework for personal data is fundamentally shaped by the EU. It seeks to walk the fine line between privacy protection and fostering data sharing.

Integration of personal data is a strategic consideration for all future-oriented banks. This will be driven by the underpinning regulatory regime, but also by the viability of technology, and – even more – by clients who expect a smooth and tailored approach that respects their privacy. With regard to the regulatory framework, we recommend the EU to:

- **Create a coherent framework for access to personal data.** Policy-makers should consider expanding the existing open access regime beyond the realm of payment data, to other personal data. A blueprint for this is provided in this viewpoint (Box 1).
- **Encourage cooperation between data protection authorities.** This will be important to achieve the implementation of the single rulebook in the data economy.

1) A coherent EU framework for personal data

Two crucial pieces of the new personal data architecture are being rolled out across the EU – the second Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR).

The GDPR is a landmark personal data protection framework that is arguably the world’s most stringent. It gives customers the right to receive their personal data upon request and for their data to be directly transmitted to third parties.

PSD2 meanwhile implies that banks must share customers’ payments data – with the customers’ explicit consent – with other regulated entities in real-time. Whereas the scope of data that can be shared under the GDPR is wider than under PSD2, GDPR neither mandates a standardised format or real-time sharing.

In today’s data economy, the boundaries between sectors are increasingly blurred. This is pertinent for the banking sector, where technology companies are looking to set down their marker.

Whilst we support the open architecture philosophy of PSD2, we believe there is an un-level playing field between banks and their non-bank competitors as regulated open access only applies in one direction.

On the condition that strong safeguards remain in place, we believe the EU should focus on extending the open access regime for personal data pioneered by PSD2 to other sectors to ensure a more coherent framework. This should, in particular, focus on the role of online platforms. The first opportunity to address this asymmetry is the European Commission proposal for a Platform-to-Business Regulation.

Box 1: customer data in the EU

- **Consent** – personal data can only be shared with explicit consent from the data owner. Consent can be retracted at any point.
- **Access** – subject to customer consent, access to personal data should only be given to regulated entities on a continuous and non-discriminatory basis.
- **Use of data** – should always serve the clients interest.
- **Liability** – a strict regime in place that is clear and easy for consumers to navigate.
- **Transparency** – clear and transparent communication about how and for what purpose payments data is used.
- **Cybersecurity and data protection** – regulated entities using data must comply with the applicable cybersecurity and data protection rules. This includes being transparent to customers about their data and respecting data retention periods.

2) Cooperation between authorities and harmonisation of the EU's regulatory landscape

To turn the EU into a cross-border data economy, regulatory fragmentation should be tackled. Since the 1995 Data Protection Directive, all EU countries have national authorities that monitor compliance with data protection laws. However, as the Directive was transposed differently in national laws, discrepancies in interpretation between national authorities have flourished.

We welcome the establishment of the European Data Protection Board under the GDPR, which was set up to help counter such fragmentation. Here, the PSD2 regime can draw lessons from GDPR, as the supervisory landscape for payments remains fragmented, with four authorities in the Netherlands alone being involved in its oversight. Given this is multiplied across countries, it remains difficult to offer cross-border products.

Looking across EU legislation, recent regulatory reforms touching on personal data (such as GDPR, PSD2, but also the Anti-Money Laundering Directive (AMLD)) will produce either overlap or conflicts. This shows that cooperation between regulators should extend beyond legislation-specific issues.

Fostering supervisory convergence across competent authorities is a goal that should be pursued by the EU.

Conclusion

We believe the EU should consider expanding the open access regime pioneered by the PSD2 to – in first instance – platforms, followed by other sectors, while keeping strong safeguards for our customers, such as the GDPR, in place. At the same time, the EU should stimulate better coordination between authorities and further harmonise EU rules. This would create a safe environment for the data economy and level the playing field between sectors.

One way of doing so would be through an oversight framework, obliging authorities to cooperate with counterparts in other Member States in order to foster a coherent understanding of the rules.

This will make it easier to service clients across borders and reduce the potential for regulatory arbitrage. Whilst ambitious, the European Data Protection Board, but also the European Supervisory Authorities (ESAs), offer valuable blueprints for enhancing implementation of the single rulebook in the data economy. Based on this approach, the EU will also be better positioned to shape the nascent international debate on data issues.

Box 2: the value of data

The digitalisation of financial services is strongly driven by data. This bears both challenges and opportunities. In the new digital reality, customers expect more tailored services that keep their data secure. Building expertise in analysing data is helpful in various ways:



Cybercrime and fraud



Process efficiency



Client expectations

In addition to understanding customer needs better, improved access to data will help banks to meet the expectations of policy-makers, regulators, and society as a whole. Policy-makers expect banks to help in the fight against financial crime, in particular preventing money laundering and terrorist financing and improving risk management functions. Access to customer data can help banks meet those expectations.

Case study: meeting client expectations through pre-approved or on-demand consumer loans

When customers need a loan, they do not want to spend time providing supporting documents and filling in lengthy credit application forms. They expect the loan process to be simple, intuitive, and effortless.

To meet this expectation, algorithms are used. These algorithms process information such as customer transactions, banking products, savings, income and payments. Combining this internal information with external information and data science provides an estimate of the customer's income and expenses. This together with other data used in the credit scoring process allows banks to prepare a personalised, pre-approved or on-demand offer.

By using personal and non-personal data, banks can improve responsible lending practices. This in turn ensures lower default rates, prevents over-indebtedness, is more efficient, and creates a better customer experience.