SHORTCOMINGS OF THE EU PROPOSAL FOR FREE FLOW OF DATA

The EU legislator has proposed banning mandatory non-personal data localisation to help unlock the data economy. While facilitating the free flow of such data within the EU is laudable, the proposal has a number of shortcomings, writes **CATHAL FLYNN**

On 19 September 2017, the European Commission published a proposal for a new regulation prohibiting mandatory localisation requirements for non-personal data in the EU.[1] The importance of this proposal to achieving a competitive data economy in Europe is reflected by the member states' decision to prioritise it for legislation. On 19 December 2017, the European Council published a revised text of the proposal[2] and decided on a mandate to begin negotiations with the European Parliament as soon as possible.

Despite the significance attached to it, there are a number of shortcomings to this legislative initiative. First, the Commission has failed to make a convincing case for legislating on the free flow of non-personal data in the EU. The key premise underpinning the draft regulation is that mandatory data localisation restrictions are unduly hindering cross-border data flows at a significant cost to the information and communications industry (ICT) sector and wider European economy. The Commission has failed, however, to adequately identify the nature and scale of this problem in its impact assessment of the regulation.

Second, there is some ambiguity in respect of the actual scope of application of the regulation. Under the current wording of the Commission and Council drafts, the application of the regulation would be determined purely in relation to the character of the data. This contrasts with the discussion in the impact assessment report, which assumes a broader scope of application based on the type of localisation requirement enacted in respect of the data. There is a substantial difference between both approaches. It is submitted that, as currently worded, the draft regulation risks creating a dichotomy in terms of the regulation of personal and non-personal data flows within the EU that would give rise to the conceptual and operational challenges described in this article.

Third, the proposed legislative framework for facilitating cross-border access to non-personal data is unsatisfactory. The Commission and Council have not addressed the possibility that direct disclosure of data to a competent authority from one member

state could be prohibited in the member state where such data is actually located. The draft regulation may therefore give rise to legal uncertainty for service providers in the EU. Moreover, the draft fails to establish sufficient safeguards around such access, including in relation to fundamental rights protection. These shortcomings call into question both the wisdom of the Commission's proposed principles-based approach and the appropriateness of legislating on the sensitive issue of cross-border data access under an instrument aimed primarily at EU economic market integration.

This article briefly discusses mandatory data localisation requirements and describes how they can impact negatively on the ICT sector and the wider economy. The key principles of the draft regulation are then discussed. This is followed by a critical analysis of the proposal, focusing on the three shortcomings outlined above. A number of conclusions are then presented.

WHAT ARE MANDATORY DATA LOCALISATION REQUIREMENTS?

Data localisation restrictions dictate or influence the localisation of data for its storage or processing.[3] These types of restrictions come in many forms, from hard law to soft law measures and administrative practices. An example of a localisation restriction would be a legislative requirement that certain types of data (for example, financial or health data) generated in a particular country or relating to that country's residents, citizens or incorporated entities be processed and stored in that country.

The number of data localisation restrictions enacted at the national level has been increasing in response to a combination of factors, including the digitisation of the global economy and the development of cloud computing. For example, Russia and China passed legislation establishing data localisation requirements in 2014 and 2017 respectively and similar laws have been enacted in several other countries. Within the EU, more than 60 restrictions have been identified across 25 member states, but the Commission believes there may be many more.[4]

The reasons why states enact data localisation requirements are explored briefly below (and see also panel overleaf for disadvantages).

● **Security.** Mandatory data localisation requirements can be driven by data security concerns, including those relating to confidentiality, integrity, continuity and accessibility. As noted by the Commission in its impact assessment report accompanying the draft proposal, states may require local processing and/or storage as a means of protecting the confidentiality of certain types of data and to control access to such data. This could relate specifically to citizens' data, national sensitive data, privileged information and industrial secrets.[5]

More broadly, security related concerns can also give rise to legitimate customer preferences for local storage. This is likely to be the case if there is a perception that the data would be subject in the country of origin to stronger security safeguards and stronger substantive and procedural safeguards in respect of law enforcement access (see "surveillance").

> **The number of data localisation restrictions enacted at the national level has been increasing.**

● **Surveillance**. The globalised nature of ICT service provision triggers complex data dislocation scenarios where information originating in one country is potentially exposed to the laws and jurisdiction of one or several other countries. This challenge has been compounded by the fact that cloud service provision can involve the storage of data redundantly in multiple copies to safeguard against loss or inaccessibility should a server (or data centre) malfunction.

This phenomenon presents significant challenges for law enforcement authorities seeking direct access to electronic evidence for national investigation purposes. States have sought to address these challenges in a number of ways, including through the imposition of mandatory data localisation requirements. As a practical matter, the ability of a law enforcement authority to procure direct access to data will depend to a large extent on the localisation of that data within the same territory. Mandating data localisation therefore guarantees law enforcement authorities direct access to that data.[6]

● **Economic protectionism.** Mandatory localisation requirements invariably place multinational service providers at a disadvantage to their local counterparts or competitors. In practice, such requirements necessitate the deployment by a cross-border service provider of a data hosting capability at the local level where such deployment may not otherwise have been required. This contrasts with the situation for local service providers that are focused on their own national market and that would, in all likelihood, have to arrange for a data hosting capability in-country in any case. This distinction may, however, be less relevant with the onset of the cloud.

THE DRAFT EU REGULATION

The key points in the draft regulation are as follows.

● **Safeguarding the free flow of non-personal data across borders.** Article 4(1) of the draft prohibits member states from obliging service providers to locate the storage or processing of electronic "data" within their borders, unless justified on grounds of "public security". Any such public security grounds would need to be expressly justified and notified to the Commission under Article 4(2) for assessment and approval. Article 4(1) is aimed at catching both direct data localisation requirements and measures having equivalent effect. The regulation as a whole, including Article 4, applies in respect of activity taking place within the EU only.

The term "public security" is not defined in either the Commission or Council drafts. However, Recital (12) to the Commission and Council drafts

NEGATIVE CONSEQUENCES OF MANDATORY DATA LOCALISATION

Mandatory data localisation can have a number of negative consequences. These are as follows:

- There are concerns that these requirements can be used to facilitate domestic surveillance that would not otherwise be possible where data is exported. It has been argued that this can be achieved in two ways. First, the storage of data in local servers significantly enhances the chance of domestic authorities acquiring direct access to that data. Second, and less obviously, the ability to procure direct access to data stored locally in this manner can be used by national law enforcement authorities as a bargaining chip when negotiating with third country authorities for the sharing of data stored in their jurisdiction.[7]
- Data localisation requirements raise important issues in respect of trade. These requirements can be used for economic protectionist purposes to place multinational or foreign service providers at a disadvantage to their local competitors in the manner described earlier in this article. They can constitute barriers to market entry and disrupt continued service provision in specific geographies. There is increasing recognition of the negative impact of national data localisation requirements on global trade. For example, these measures have been called out in 2017 by the US Trade Representative as a "key barrier to digital trade".[8]
- Compliance with mandatory data localisation can be costly for service providers, particularly start-ups, and can lead to the otherwise unnecessary multiplication of data storage and processing activities and facilities.[9] This can lead to distorted markets for cloud service providers. As noted by the Commission in its impact assessment report on the draft regulation, data localisation requirements force these types of service providers to make business and investment decisions that lead to "suboptimal" outcomes in cost, security and operational agility.[10]
- Mandatory data localisation risks leading to a loss in growth and innovation potential. This is because data localisation restrictions form barriers to new types of services that are geographically distributed by design and truly global in nature. The deployment of internet of things (IoT) services is cited by the Commission as a particular risk in this respect.[11] The Council also explicitly acknowledges the importance of IoT as a source of non-personal data in the new Recital (10a) that it has inserted into the draft regulation.
- Finally, there are concerns that, by leading to a combination of the above, such practices could risk undermining the internet's innovative potential.[12]

clarifies that this concept should be understood within the meaning of Article 52 of the Treaty on the Functioning of the European Union (TFEU). The newly inserted Recital (12a) to the Council's draft develops this concept.

The term "data" is defined in the Commission and Council drafts as data other than "personal data" as defined in Article 4(1) of the General Data Protection Regulation (GDPR). However, neither the draft regulation itself, nor its explanatory memorandum, explicitly identify or provide examples of the types of "data" (or "non-personal data") that would be covered under this legislative proposal. Annex 5 to the Commission's impact assessment report makes various references to the following types of data: public and government data, tax, accounting and company data, gambling data, financial data, telecoms data and health data.[13] Annex 6 lists data localisation requirements and their obligations per member state which cover these same areas. The intention therefore appears to be that the regulation will apply in respect of these types of data, although it is difficult to see how at least some of these would not constitute personal data within the meaning of Article 4(1) of the GDPR.

- **Data availability for "regulatory control".** Articles 5 and 7 of the draft are aimed at facilitating cross-border access to non-personal data by competent authorities. The latter term is defined very broadly under Article 3(6) of the draft as any member state authority (and, in the Council's draft, "any other entity authorised by national law to perform a public function or exercise public authority") that has the power to obtain access to data for the performance of its official duties under national or EU law.

  Specifically, Article 5(1) provides that the regulation shall not affect the powers of competent authorities to procure direct access to data. It also provides that direct access to data may not be refused on the basis that such data is located in another member state.

  The remainder of Article 5, together with Article 7, establishes a framework under which a competent authority from one member state can request the assistance of a competent authority from another member state to procure access to non-personal data. Certain differences exist between the Commission and Council drafts in relation to how this framework will operate in practice. However, both institutions are in agreement that cross-border access should only be granted by one member state to another where no specific cooperation mechanisms exist between both countries.
- **Cloud services portability.** Article 6 of the draft regulation encourages and facilitates the development of self-regulatory codes of conduct at EU level to facilitate user switching between service providers of cloud storage and porting data back to users' own IT systems. This initiative takes account of Article 20 of the GDPR, which gives the data subject the right to receive the personal data concerning him/her from a data controller and the right to transmit that data to another controller.

SHORTCOMINGS OF THE DRAFT REGULATION

It is submitted that the draft regulation has three shortcomings that give rise to a number of substantive concerns. These are discussed below.

Failure to make a strong case for legislating on this issue. The nature and scale of the problem that the Commission is seeking to address with this legislative initiative is not clear. This lack of clarity was identified by the Commission's Regulatory Scrutiny Board (RSB) as one of the principal shortcomings of the Commission's September 2017 proposal in its second negative opinion on the legislative initiative.[14] More specifically, the RSB concluded that the impact assessment report accompanying the draft proposal fails to establish the size of the problems of location restrictions on non-personal data.

The RSB also contends that the impact assessment

report fails to explore the reasons for data localisation restrictions, analyse their merits or analyse the strength of observed customer preferences for local storage. This is a significant omission considering that there may be legitimate customer preferences for local storage. This is likely to be the case, for example, if there is a perception that the data would be subject in the country of origin to stronger security safeguards and stronger substantive and procedural safeguards in respect of law enforcement access.

The Commission's decision not to address this issue is surprising considering that Annex 5 to the impact assessment report acknowledges that 60% of the IT service providers consulted prior to the publication of the draft regulation indicated that their users demand local data storage and/or processing. The Commission appraises the existence of these customer preferences in a very narrow context, however, and assumes that they arise solely as a result of a perception on the part of users that localisation requirements exist under national laws together with a preference for a risk averse approach.[15]

Notwithstanding this, the Commission goes on to concede elsewhere in Annex 5 that the users of data services display a "degree of lack of trust" in cross-border storage of data. Specifically, the Commission states:[16]

"In a survey, 30% of business respondents recognised they preferred that the data generated and used by their business is stored and processed inside the country they operate. ***Over 35% of the respondents see location as a proxy for security of data.***" (our emphasis)

There is therefore a clear inconsistency in the Commission's own analysis of customer preference in its impact assessment.

Finally, the RSB concludes that the Commission failed to make a satisfactory case for a new right of cloud service portability. According to the RSB, the Commission has not demonstrated that switching costs are excessive. It also notes that the proposed portability solution would not address the obstacles to switching identified in the impact assessment report, including standardised data formats and data transfer logistics.

Scope of application. As noted earlier, "non-personal data" is defined under the draft regulation as data other than "personal data" defined in Article 4(1) of the GDPR.[17] Personal data is defined under Article 4(1) as any information relating to an identified or identifiable natural person. This means that, as currently worded, the applicability of the draft regulation is determined purely in relation to the character of the data; i.e., whether it qualifies as personal data within the meaning of Article 4(1) of the GDPR or not. This is consistent with the discussion in the Recitals to the draft, including Recitals (9) and (10), for example.

Notwithstanding this, the Commission's impact assessment report assumes a broader scope of application for the draft regulation. According to page 5 of the report, the regulation does not concern the processing of personal data and the

> **The Commission concedes that users of data services display a 'degree of lack of trust' in cross-border data storage.**

free movement of such data "as governed" by the GDPR, Article 1(3) of which prevents member states from restricting or prohibiting the free movement of personal data within the EU for reasons "connected with the protection of natural persons with regard to the processing of personal data". Interestingly, the Commission has assumed for the purpose of this legislative initiative that Article 1(3) of the GDPR is functionally equivalent to an explicit prohibition on localisation (as established under Article 4 (1) of the draft regulation).

Under the approach described in the impact assessment report, the applicability of the regulation would be determined on the basis of the type of data localisation requirement enacted in respect of the data, as opposed to the character of that data. This would mean that national localisation requirements that apply in respect of "personal data" would also fall within the scope of the regulation, assuming that such requirements are not aimed at the protection of such personal data as contemplated under Article 1(3) of the GDPR. The report further clarifies that, where such requirements are aimed at the protection of personal data, they would be addressed by the GDPR and, as such, would fall outside of the scope of the draft regulation.

To illustrate this broader scope of application, the example is provided by the Commission of a national requirement to store corporate information locally (including registers of shareholders and directors which constitute personal data). This national data localisation requirement is aimed at enabling shareholders and other interested parties to access the corporate information, as opposed to the protection of personal data as contemplated under Article 1(3) of the GDPR. The report concludes that, because these requirements would not be addressed under the GDPR, they would be addressed under the draft regulation.

The discussion in the impact assessment report is therefore at odds with the wording of the draft regulation itself, which would allow member states to apply data localisation requirements in respect of personal data based on (for example) taxation or accounting laws that are not associated with personal data protection. At the same time, these types of requirements would fall squarely within the more extensive prohibition established under Article 4 (1) of the draft regulation where applied in respect of "non-personal data" as currently defined, assuming, of course, that they cannot be justified on grounds of "public security".

Such an outcome also appears inconsistent with the EU legislator's stated objective of creating a single EU dataspace with a coherent set of rules for the free movement of different types of data. There is a risk that the draft regulation could create an incongruity regarding the regulation of different types of data flows within the EU. Specifically, data that does not qualify as personal data would be subject to the broad localisation prohibition established under Article 4 (1) of the draft regulation (with the exception of data localised for "public security" purposes), while all personal data would be subject to the prohibition on restricting or prohibiting free movement established under Article 1(3) of the GDPR that applies only in respect of measures aimed at personal data protection.

This incongruity would create certain operational problems for service providers. The Commission has stated in the impact assessment report that, to the extent that the proposed regulation would deal with mixed data sets that include personal data, the applicable provisions of the GDPR must be fully complied with in respect of the personal data part of the set.[18] This principle has been worked into the draft itself as part of the Council's amendments to Recital (10) that are aimed at clarifying the relationship between the draft regulation

and the GDPR. Accordingly, Recital (10) states that, where non-personal and personal data are "inextricably linked", the draft regulation should not "prejudice the application of [the GDPR]". Recital (10) also states that the draft regulation does not "impose an obligation to store different types of data separately".

Assuming that the scope of application of the draft regulation is determined on the basis of the current definition of "non-personal data", member states would be free to require localisation of the personal data part of a mixed set (where this requirement is not based on the protection of such data) but prohibited from doing so with regard to the non-personal part of that set (unless on grounds of "public security"). This calls into question the validity of the Council's statement under Recital (10) that the draft regulation does not impose an obligation to store different types of data separately. The potential difficulty here is perhaps implicitly acknowledged later in the Council's draft, Recital (28) of which allows the Commission to periodically assess "the experience gained in applying [the regulation] to mixed data sets".

The broader scope of application contemplated in the impact assessment report (whereby the applicability of the draft regulation would be determined on the basis of the type of localisation requirement enacted in respect of data, as opposed to the character of that data) eschews the conceptual and operational challenges described above. This approach would achieve a consistent regime for regulating personal and non-personal data flows in the EU whereby all personal data in the EU would be subject to either:

- The limited prohibition on restricting or prohibiting free movement established under Article 1(3) of the GDPR (assuming, as the Commission does, that this is functionally equivalent to an explicit prohibition on localisation);

or, where a member state localisation requirement is not aimed at the protection of personal data,

- The more extensive (and explicit) prohibition on localisation established by Article 4(1) of the Commission's draft regulation that also applies to data other than personal data.

This approach is also in line with the Commission's earlier discussion in its communication on building a data economy from January 2017 where it distinguishes between restrictions to the storage and processing of personal data justified on the grounds of personal data protection, and restrictions justified on other grounds that "need to be assessed on the basis of [...] EU legal instruments [other than the GDPR]".[19]

Proposed framework for cross-border access to non-personal data. The Commission has chosen a principles-based legislative cooperation framework over a more detailed and prescriptive approach. This has given rise to the following concerns regarding the provisions in the draft regulation aimed at facilitating cross-border access to data.

- First, Article 5(1) of the proposal provides that access to data may not be refused on the basis that it is "[stored or otherwise] processed in another member state".[20] It is assumed that this provision is directed at the service provider that will be subject to a request for access.

The possibility that the disclosure of data to a competent authority in one member state could be prohibited in the member state where such data is actually stored or otherwise processed has, however, not been addressed under Article 5(1). Therefore and to avoid any risk of legal uncertainty, Article 5(1) should also provide that a service provider will not be in breach of the law of one member state when complying with a request for access from another member state.

The associated risk faced by service providers in this regard is augmented under the Council's draft, which, under a new Article 5(3a), provides for the imposition of sanctions for failure to comply with a request by a competent authority pursuant to Article 5(1).

- Second, guidance would be welcome in respect of the circumstances under which a competent authority can legitimately request the assistance of another member state for access to data under the draft regulation. Reference is made, under Recital (18) and Article 5(2) of the Commission's draft, to the competent authority "[exhausting] all applicable means to obtain access to [such] data". However, no clarification or guidance is provided by the Commission on how onerous this standard of exhaustion of "all applicable means" should be.

> **"It is unclear what safeguards would be applied for procuring cross-border data access."**

The Council's draft dispenses with this construct altogether (in fact Article 5(2) is removed completely from that version and the relevant wording discussed above is struck out of Recital (18)).

Instead, the Council proposes that a member state be allowed to request assistance from another member state where it "does not receive access pursuant to [Article 5(1)]". This implies a lower threshold to be met by competent authorities before they can make a legitimate request for assistance under the regulation. Again, guidance would be helpful.

- Third, and related, it is unclear what substantive safeguards (if any) would be applied when a member state does request another member state for assistance to procure cross-border data access.

For example, the Commission and Council drafts are silent as to whether a request for assistance from one member state to another must respect the rule of law or fundamental rights as established under the EU Charter of Fundamental Rights, including the right to liberty and security (Article 6), the right to privacy (Article 8) (assuming that the draft Regulation will also apply in principle to personal data) and some of the rights established under Chapter VI (Justice).

The only substantive requirements established in the Commission's proposal can be found under

Recital (18) and Article 7(3). Recital (18) provides that the requested member state can refuse to grant assistance to the other member state if doing so would be contrary to its "public order". Article 7(3) requires that the request for assistance be "duly motivated" and include a written explanation of its justification and the legal basis for seeking access. The Council's December 2017 draft retains Article 7(3). Significantly, however, the Council has removed the wording under Recital (18) that allowed a member state to refuse a request for cross-border access on "public order" grounds.

Recital (18) of both the Commission and Council drafts does provide that, when requesting assistance, member state authorities should "use" cooperation instruments established under EU or international law. A number of such instruments are explicitly cited in Recital (18), including, for example, framework decision 2006/960 and directive 2014/41/EU of the European Parliament and Council establishing a framework for the European Investigation Order (EIO) in criminal matters.

It is not clear, however, the extent to which any substantive safeguards established in these instruments would be applicable in respect of the cross-border data exchanges contemplated under the draft regulation and, assuming that they are, whether they would be appropriate in practice.

Article 7(6) of the Commission's draft provides that the Commission may adopt implementing acts setting out details of the procedures for requests for assistance. This would leave open the possibility for the Commission to address some of the shortcomings described above in the future. Whether or not it is appropriate to grant the Commission this measure of discretion in respect of such a sensitive issue is another matter. This may, in any case, be a moot question as the Council has removed Article 7(6) from its draft. This would suggest that the Council considers that the regulation is capable of operating on its own and without the benefit of implementing acts. As shown above in the context of cross-border access to non-personal data, this is questionable.

As a general observation, the substantive shortcomings described above raise questions about the wisdom and indeed appropriateness of including a framework on cross-border access to data in the draft regulation in the first place. The inclusion of these provisions is clearly aimed at alleviating member states' concern that the draft regulation would undermine their ability to procure direct access to non-personal data. This is acknowledged by the Commission in the impact assessment report where it states that the availability of data for regulatory control emerged during the structured dialogue preceding the publication of the draft regulation as a "key concern"[21] for member states. The report also states that the availability of data in this manner was identified as a:

"[...] 'functional requirement' to flank a potential free flow of data right: member states indicated to be willing to remove certain data localisation restrictions if availability of certain data would be guaranteed by another provision of the legal act."[22]

The Commission has therefore sought to create a type of quid pro quo in that, while the draft regulation prohibits mandatory data localisation requirements on the one hand, it makes it easier for the member states to procure cross-border access to data on the other. The Council, in turn, has sought to strengthen the proposed framework for cross-border data access where possible through a number of important amendments to the Commission's original draft, some of which are controversial and have been discussed above.

This quid pro quo has, however, required that the sensitive issue of cross-border data access be addressed as a secondary issue in a legislative instrument primarily aimed at achieving economic market integration within the EU. It is submitted that, precisely for the reasons discussed above, this approach has led to an unsatisfactory outcome.

One final remark on the choice of legal basis. The draft regulation is based on Article 114 of the TFEU, which allows for the harmonisation or approximation of national laws for the creation of an internal market. The Court of Justice of the EU (CJEU) has considered the relationship between surveillance related requirements and the regulation of economic activity within the EU when determining the suitability of Article 114 of the TFEU as a legal basis under EU law.

In 2006, Ireland (supported by Slovakia) challenged the Commission's choice of legal basis for the (now annulled) EU Data Retention Directive. Both countries argued that the then Article 95 of the Treaty establishing the European Community (current Article 114 of the TFEU) was an inappropriate legal basis for the EU Data Retention Directive as the latter's main objective was not to eliminate barriers and distortions in the internal market but to harmonise the retention of personal data to facilitate action by the member states in criminal law. The CJEU rejected this argument in a 2009 judgment and ruled that the legal basis chosen by the Commission was appropriate. The CJEU subsequently held that the Data Retention Directive was unlawful on grounds of fundamental rights protection in a separate ruling from 2014.

CONCLUSION

Despite the significance attached to it, there are a number of shortcomings to the EU's draft regulation on the free flow of non-personal data. It is hoped that they can be remedied by the co-legislators as the draft progresses to the European Parliament, although it is unclear at this stage how co-legislators will reconcile the competing issues of data sovereignty, a consistent approach towards data free flow, and fundamental rights protection explored in this article.

CATHAL FLYNN *is an Irish qualified barrister (non-practising) and specialist in communications regulation in the tech and comms group at Bird & Bird in London. Email: cathal.flynn@twobirds.com. This article does not constitute legal advice.*

REFERENCES **1** Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union. 13 September 2017. bit.ly/2wfu2sJ **2** Revised proposal, 19 December 2017. bit.ly/2CNdOWx **3** Staff working document on the free flow of data and emerging issues of the European data economy, accompanying the communication on Building a European Data Economy. SWD(2017) 2 final, p5. bit.ly/2iDu84H **4** See p37 of Annex 5 to the Commission staff working document impact assessment, citing: LE Europe study (SMART 2015/0016) and TimeLex study (SMART 0054/2016). bit.ly/2BqVk1e **5** Impact assessment, p8. See also Annex 5, pp60–61. **6** Impact assessment, Annex 5, pp59–60. **7** Hill JF (2014). The growth of data localization post-Snowden: analysis and recommendations for US policymakers and business leaders. Hague Institute for Global Justice, pp21–22. bit.ly/2BvbfJ2 **8** Office of the United States Trade Representative (2017). Key barriers to digital trade. bit.ly/2kfBeg6 **9** Impact assessment, p11. **10** Impact assessment, p12 citing: LE Europe study (SMART 2015/0016). **11** Impact assessment, p12. **12** Impact assessment, p5. **13** See e.g. Impact assessment, Annex 5, pp39, 41–42. **14** The RSB issued two negative opinions on the proposal on 28 September 2016 and 25 August 2017; for the second, see: Impact assessment for the digital single market initiative on the free flow of data. Ares(2017). bit.ly/2EV80uX **15** Impact assessment, Annex 5, p43. **16** Impact assessment, Annex 5, p61. **17** This distinction is also made in the explanatory memorandum accompanying the draft regulation, p2 of which states that the draft regulation does not affect the EU data protection legal framework as it "concerns electronic data other than personal data". **18** Impact assessment, p3. **19** Impact assessment, p10. **20** The Commission's draft from September 2017 includes the wording "stored or otherwise processed" while this wording has been removed from the Council's draft text from December 2017. **21** Impact assessment, p48. **22** Impact assessment, p48.