techUK

techuk.org | @techUK | #techUK

techUK response to the Department for Culture, Media & Sport – Call for views on the General Data Protection Regulation derogations

17th May 2017

10 St Bride Street
London
EC4A 4AD

T 020 7331 2000
F 020 7331 2040
www.techuk.org

techUK | Representing the future

About techUK

techUK welcomes the opportunity to respond to the Department for Culture Media & Sport's Call for views on the General Data Protection Regulation (GDPR) derogations. The tech sector has a long history of positive engagement with both UK Government and the European Union as the new GDPR has been negotiated and agreed.

techUK is the industry voice of the UK tech sector, representing more than 900 companies who collectively employ over 700,000 people, about half of all tech jobs in the UK. These companies range from innovative start-ups to leading FTSE 100 companies. The majority of techUK members are small and medium sized businesses.

techUK would be happy to discuss the contents of this response with DCMS further.

General Comments

There are a significant number of derogations within the GDPR legislation giving Member States some degree of flexibility in how they implement the regulation. The tech sector has long called for a consultation on how the UK Government intends to implement these derogations given they will have a significant impact on the operation of new data protection laws going forward. Industry has been promised this consultation for many months.

The contents of the call for views however does not align with expectations. The structure of the call for views and lack of policy substance creates challenges for responding. At this late stage, just over one year from the compliance deadline, and with pressing Brexit-related policy decisions pending, industry had expected a consultation outlining detailed policy options.

The Government frequently, and rightly, talks of the importance of the UK tech sector as a key driver of the economy. techUK recognises this support, however this specific call for views does not provide that opportunity for collaboration.

Following this call for views, and given the proximity of the deadline to implement GDPR, it is vital that Government further consults industry on its policy approach to these derogations. This consultation should take place prior to any implementing legislation for GDPR as, whilst it is important the Government prepare to implement the new regulation, a considered approach in collaboration with industry is also important. techUK looks forward to continued engagement as the Government considers how to implement the most significant reforms to data protection laws in decades.

Derogations and the future of UK-EU Data Flows

Since the UK voted to leave the EU, the Government has outlined an ambitious and bold vision for Global Britain, and a new relationship with the European Union. The tech sector looks forward to assisting the Government in making that vision a reality. As techUK's recent report, *'The Digital Sectors After Brexit'*[1] sets out, a truly Global Britain, built on international trade will only be possible if we have in place a robust legal basis for cross-border data transfers before we leave the EU. That is why guaranteeing international data flows, from the first day the UK's new trading arrangements with the EU come into effect is one of techUK's four top priorities for the forthcoming negotiations[2].

techUK welcomes the Government's high level commitment to maintaining the stability of data flows[3]. Among existing options achieving an adequacy finding from the EU is the most effective way to achieve this. An adequacy finding would be, particularly for small businesses, the simplest and least burdensome means of guaranteeing international data flows, ensuring minimal disruption for UK and EU companies alike.

The Government's welcome commitment to fully implement GDPR[4], as called for by techUK, should assist with negotiating a secure and robust mechanism for cross-border data transfers between the UK and EU. As part of its plan to fully implement GDPR, the UK Government should continue to lead the discussion when considering how to approach the derogations. Harmonisation should be encouraged across Member States, based on UK leadership.

Call for views Questions

Theme 1 – Supervisory Authority

Article 51 sets a provision for each Member State to assign an independent authority to be responsible for monitoring the application of the GDPR. Generally in the UK most of these provisions should remain as currently set out in Schedule 5 of the Data Protection Act 1998, however there are some aspects which should be re-considered, as set out in subsequent comments in this section.

[1] https://www.techuk.org/insights/news/item/10086-the-uk-digital-sectors-after-brexit
[2] https://www.techuk.org/insights/news/item/10089-techuk-priorities-for-european-exit-negotiations
[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf
[4] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/responsibilities-of-the-secretary-of-state-for-culture-media-and-sport/oral/42119.html

Article 52 (4) and 52 (6) refer to resourcing and financing of the national supervisory authority. The Government must consult with industry as to the approach it intends to take for financing the ICO once notification fees are removed under the GDPR. **It is crucial that the funding structure is not based on fines.** The ICO must remain impartial and objective in its enforcement activities, and should not be inappropriately incentivised to enforce by virtue of its fining powers.

Article 53 (1) allows Member States to determine how their supervisory authority is appointed. **The Government should consider making the ICO accountable to Parliament**, rather than the Department for Culture, Media & Sport, to ensure transparency, accountability and independence.

Article 58 (1)(f) allows access to the premises of the controller and the processor, in accordance with Member State law. If the Government is intending to amend existing UK legislation, in line with the Data Protection Act 1998 and Coroners and Justice Act 2009, it should consult on the circumstances and types of investigations where this power would be proportionate and necessary-- specifically given the significant commercial disruption to businesses that search and seizure powers would cause. Search and seizure should only be used where such action is justified, such as following persistent, documented non-cooperation.

Article 58 (6) allows Member States to provide additional powers to the supervisory authority. The Government should consult with both the ICO and industry if it is considering giving additional powers to the ICO. However**, techUK believes that, given the powers already granted by the GDPR, no additional powers would be necessary**.

Article 62 outlines the approach supervisory authorities should take when conducting joint operations. In legislation the Government should be clear that the jurisdiction of the ICO is limited to breaches by UK-registered data controllers/processors, and how the ICO could engage in enforcement in situations where infringements with a nexus for UK jurisdiction also involve other jurisdictions. These operations should take place according to a clearly defined structure that is transparent to data controllers and follow the principles of due process.

Article 90 and **Article 54 (2)** set out secrecy obligations. GDPR implementing legislation should include specific provisions which require the ICO to protect and respect commercial confidentiality. This is currently missing in the Data Protection Act 1998, and does not appropriately constrain the ICO from disclosing commercially sensitive information. This anomaly should be rectified in new primary legislation. This could be based on the provisions in Article 10 (1) of the Second Schedule of the Irish Data Protection Act 1988, or similar provisions

which apply to other regulators. This obligation should apply in particular to all investigations carried out by the ICO as well as information shared under the obligation to consult about 'high risk processing', which is likely to take place prior to launching a new product or service to market. Cooperation with other data protection authorities under **Article 61 (4)(b)** should not undermine this confidentiality requirement. The ICO should have an affirmative duty to ensure that it only shares commercially confidential information with other authorities where explicitly required in law (i.e.: non-discretionary) and that those authorities are bound by the ICO to respect the same rules on commercial confidentiality.

Theme 2 – Sanctions

Article 36 (5) allows Member States to determine whether prior authorisation is necessary for processing by a controller for the performance of a task carried out by the controller in the public interest. **techUK believes that no prior authorisation should be necessary**, but Government should share its thinking if it is considering taking a different approach and consult with industry on options.

Article 58 (4) refers to effective judicial remedy and due process for supervisory authorities exercising their powers. The ICO should be bound by existing UK laws which set out effective judicial remedies and due process. Any proposals to change this must be consulted on and clearly set out appropriate triggers and thresholds. **As a matter of principle, recourse to Courts should be a last resort.** The system should avoid creating an environment which encourages vexatious claims or abuses of data protection law to bypass or undermine other statutes.

Article 83 (8) requires Member States to set out appropriate procedural safeguards when supervisory authorities implement fines, including effective judicial remedy and due process. This is an incredibly important check; **primary legislation should set out the fining powers of the ICO under GDPR and what factors should be considered by the ICO when considering fines**, as set out in **Article 83 (2)**. This should include aspects such as level of cooperation by the organisation, remedial action taken, impact on/harm caused to data subjects, the type of data involved and the magnitude of a breach (i.e. number of data subjects affected). The UK Government should commit to this provision in full and maintain that commitment once the UK has left the EU.

The forthcoming Bill creates an opportunity to set out a sanctions framework that minimises the risk of vexatious claims against organisations, for example by leaving lacunae in the law which allow a new industry of 'class action' lawsuits to emerge. The ICO's approach to date of guiding and actively supporting data controllers to comply with data protection law must

continue, and would be the most appropriate route to achieve the ambitions of the GDPR to create culture of privacy within organisations. Any move towards a more confrontational approach would be counter-productive in our view and should be discouraged.

It is also important that under Article 83 (8) the Government ensure organisations have the ability to challenge administrative fines and have the matter decided by a tribunal or court. This is a vital check on the GDPR's enhanced fining powers, to ensure they are not used inappropriately or excessively. Indeed, it would be most appropriate for any fines assessed by the ICO to be first reviewed by a court to determine whether they are proportionate and fair.

Article 84 requires Member States to set out penalties which do not fall within the administrative fines pursuant to Article 83. The Government should not set out any additional penalties outside the administrative fines set out in Article 83 as the sanctions outlined in the GDPR are sufficient to achieving the purpose of deterrence. If it decides to, it must consult with industry.

Theme 3 – Demonstrating Compliance

Article 40 sets out provisions for the development of Codes of Conduct to demonstrate compliance. techUK welcomes scope in the GDPR for the development of codes and other initiatives which can enhance and complement user privacy but the prescriptive nature of a Regulation has limited the space for such initiatives to develop. Government must ensure that nothing in the implementing Bill further reduces opportunities for initiatives in the public interest to emerge. Government's policy decisions in this area must also acknowledge that the successful self-regulatory code schemes are typically industry-led (rather than imposed by regulators) and often complement the regulatory framework (e.g.: enhancing user education or control) rather than serve as mechanisms for compliance with data protection law (which is the intention behind Art 40). There should therefore remain space for such codes to develop where sectors see value in creating them, and the Bill should make clear that it is for the code owners to submit a code for approval by the ICO under the legal framework rather than for the ICO or another regulator to have powers to appropriate a third party code and opine on its suitability as a compliance tool. The European Interactive Digital Advertising Alliance Code is an example where a code was developed to provide users with information about digital advertising but was not itself a data protection compliance tool.

The comments above are also relevant to **Article 41** which similarly refers to the development of certification mechanisms.

Theme 4 – Data Protection Officers

Article 37 (4) allows Member States to set out additional circumstances whereby a Data Protection Office must be appointed. **The Government should avoid going further than the already inflexible provisions set out in the regulation.** We would counsel against extending requirements which mandate the appointment of Data Protection Officers beyond the types of organisations already set out in the regulation. This would disproportionately impact small and medium sized businesses in particular.

Article 38 (5) states that data protection officers shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law. **techUK would not support further legislation requiring DPOs to maintain secrecy or confidentiality as this could create conflicts of interests with their employers.** DPOs must be able to communicate openly within their organisations.

Theme 5 – Archiving and Research

Article 89 (2) allows for derogations from the rights in Articles 15 (Access), 16 (Correction), 18 (Restriction) and 21 (object) for research or statistical purposes. **The Government should invoke this derogation by maintaining the research exemption in Section 33 of the Data Protection Act 1998.** This would prevent a barrier to innovation and allow organisations to conduct big data analytics, modelling and statistical analytics which do not lead to decisions or measures about individuals, or which do not cause damage or distress. They could do this without having to consider that data in requests to exercise the rights listed under the relevant articles. This could be particularly useful in machine learning where it can be impossible to extract the specific data of an individual. Access to information has significant benefits, encouraging learning, innovation and growth.

Theme 6 – Third Country Transfers

Article 49 refers to third country transfers. As highlighted at the start of this response, unhindered data flows are crucial for the UK economy and the Government should ensure that data can flow between the UK, the EU and other parts of the world.

Article 49 (4) sets out provisions for the transfer of personal data to third countries for important reasons of public interest. It is for Member States to determine what constitutes public interest. The UK Government must set out and consult on what are considered 'important reasons of

public interest'. Any restrictions must be the exception not the rule, and be specific, targeted and clearly set out in primary legislation.

Article 49 (5) sets out provisions for a Member State to, for reasons of public interest, expressly restrict and set limits on data transfers of specific categories of data to third countries where an adequacy decision is absent. **techUK advocates for rules which ensure the frictionless free flow of data across Europe and supports forbearance from data localisation laws across the EU.** To support its goals to grow the UK's digital economy up to and beyond Brexit, Government must adopt a bias towards the free flow of data and only intervene to restrict flows where necessary and proportionate. The free flow of data has the opportunity to add 8 billion euros[5] to the EU economy, according to the European Commission's own Impact Assessment as part of its 'Building a European Data Economy' Communication. techUK recently responded to the European Commission's communication consultation, outlining the importance of removing data localisation laws, a copy of which is annexed to this response.

Theme 7 – Sensitive personal data and exceptions

Article 9 (4) allows Member States to introduce further conditions with regard to the processing of genetic data, biometric data or data concerning health. **We do not believe the Government should seek to place additional restrictions on the processing of these categories of data, as the GDPR already provides appropriate protections, namely that the data controllers must obtain explicit consent in order to undertake processing of this data.** The processing of these categories of data are vitally important to the ability of individuals to obtain services, and for data controllers to fulfil these purposes. The implementing Bill must not constrain those services requested by the user which require the processing of special categories of data. For example a user may enter a health query into a search engine. The search engine will have to process that data in order to deliver the search results expected by the user. Similarly, devices such as fitness trackers, biometric identify products and services or DNA genetic testing kits will need to process health, biometric or genetic data in order to deliver the sole purpose of the product.

While this derogation is limited to biometric, genetic and health data, there are existing UK conditions for processing sensitive data that are not health related, but should be maintained. Those include the following:

[5] http://europa.eu/rapid/press-release_IP-17-5_en.htm

- Data Protection Act 1998 - Schedule 3
    - 7 - administration of justice
    - 7A - fraud prevention (this is particularly crucial to many businesses)
    - 9 - race or ethnic origin for equality of opportunity monitoring

- SI 2000/417:
    - Prevention or detection of an unlawful act in the public interest
    - Protection of the public against dishonesty or malpractice in the public interest
    - Combination of 1 and 2 in relation to the special purposes
    - Political opinions for legitimate political activities
    - Research purposes (as per section 33 DPA 98) in the public interest
    - Functions conferred on a constable by any rule of law

- 2002/2905 as amended by SI 2010/2961: elected representatives
- SI 2009/1811: prisoner information to inform an MP about the prisoner and arrangements for the prisoner's release
- SI 2012/1978: Hillsborough disaster: this is wider than health and may or may not continue to be needed.

In addition the Government should make clear that personal data relating to deceased persons are not sensitive data. Additionally there will be situations in which employers will have to process sensitive data.

Theme 8 – Criminal Convictions

Article 10 refers to the processing of personal data relating to criminal convictions and offences. Under the GDPR, this type of personal data is no longer part of the wider list of sensitive personal data. **The Government must make sure that there are sufficient lawful bases for processing criminal offence data, such as the fraud prevention one currently found in Schedule 3 of the Data Protection Act 1998, and whether this is sufficient** to ensure that legitimate uses of this data can continue.

Theme 9 – Rights and Remedies

Article 17 (3)(b) refers to the right to erasure and exemptions where a legal obligation exists under Member State law. The UK Government will have to consider how the UK's wider legislative landscape will impact on this derogation, including the UK's legal and policy commitment to freedom of expression. techUK supports the maintenance and reinforcement

of webmaster notice requirements which improve the effective implementation of 'the right to be forgotten'. **There is no need for additional domestic law as Article 17 (1) establishes a strong 'right to be forgotten' balancing this against other rights such as freedom of expression and information.** The UK should suggest other Member States avoid introducing additional laws in this area to achieve a balanced picture.

Article 22 (2)(b) provides Member States with a derogation which could provide an exemption to the Article 22 (1) right not be subject to a decision based solely on automated processing. techUK do not believe there is a case for additional legislation in this area; however if the UK Government is minded to utilise this derogation it must not have the effect of broadening the limitations on profiling in Article 22 (1) beyond decisions 'solely' based on automated processing and producing legal effects or similarly significant effects. This would have a devastating impact on services, including government services, which are personalised to user interests.

Article 80 (2) would allow Member States to allow any organisation to submit complaints independent of an individual data subject if it feels the requirements of the regulation are being infringed. This could lead to 'class action' lawsuits of the type discussed earlier, leading to vexatious claims not inconsistent with the goals of the Regulation or which seeks to abuse data protection law as a means of circumventing stricter tests in other statutes. This would also place additional burdens on organisations over and above the extensive requirements of this regulation, in having to deal with these complaints from organisations which have not received a specific request from a data subject. In this situation the perceived risk of processing data would increase if there was a highly litigious atmosphere. Any complaints brought forward on behalf of data subjects should be appropriate and proportionate. Most importantly **techUK urges the Government to prioritise the complaints brought by individual data subjects, who are most able to articulate alleged harms, over complaints brought by organisations who are less well positioned to represent the actual concerns of the data subjects**. Careful consideration should be given to whether to appoint such a body and which body it might be. The Government should consult on this.

Theme 10 – Processing of Children's Personal Data by Online Services

Article 8 (1) provides Member States with the opportunity to set the age below which parental consent is required to process the personal data of a child to the age of 13. **techUK believes this is an incredibly important derogation and that the UK Government should require parental consent only for users below the age of 13.**

Invoking this derogation would allow the UK, and hopefully other EU Member States, to align with global practices. Much of this international best practice stems from the US Children's Online Privacy Protection Act (COPPA) and child safety experts, digital policy experts, anti-bullying organisations, youth organisations and educational groups, among others, all support a retaining a lower age. Given the significant amount of cross-border digital activity, harmonisation should be an objective. Indeed, one of the fundamental purposes of the GDPR was to provide a harmonised approach to data protection. Data is global and knows no borders and increasingly data protection policy requires harmonisation at the international level, rather than solely at the European level.

Online services are of societal and developmental benefits to teens. To require parental consent for all users under 16 years old would prevent individuals from benefiting from services which offer significant social and educational benefits to them. As Professor Sonia Livingstone, a respected social psychologist, has stated increasing the age of parental consent for data processing to 16 years old would have the effect of "*significantly limiting children's rights to communicate with peers, engage online with educational, health and other valuable resources, or participate in the online civic sphere.*"[6]

Allowing children over 13 years old the ability to consent in their own right to use digital services would support the Government's aims in the Internet Safety Strategy (which techUK provided early input to DCMS) by supporting the development of children's digital literacy and creating opportunities to engage children in responsible and safe use of online services while still in full-time education. An ability to take part in digital life is a crucial element of developing digital literacy and there are a number of programmes which have been developed in partnership through industry and civil society, which help children and young people develop the skills, critical thinking, knowledge, resilience and support they need to navigate the online world safely as an adult. Allowing the development of digital literacy and skills from a young age would also achieve the ambition of ensuring the UK continues to be a world leader in innovation and assist with the UK's wider digital skills gap, and the need to continue to develop a domestic digital skills talent pipeline.

In order to support the aims of the Government's Internet Safety Strategy of ensuring the UK becomes the safest place in the world for young people to go online young people need to be able to engage with digital services. There is a body of evidence to support this. For example, the 2008 Byron Review stated "*Risk taking is part of child development – part of our*

[6] http://blogs.lse.ac.uk/parenting4digitalfuture/2017/04/19/no-more-social-networking-for-young-teens/

drive to learn and to succeed. Particularly in adolescence, risk taking is not only a developmental imperative but also a lifestyle choice: it is driven by developments taking place in the brain and it is an important part of identity construction. Taking risks is something children need to do to reach self-actualisation (the process of fully developing ones personal potential which is described in Maslow's Hierarchy of Needs, see figure opposite) and most children get pleasure from taking risks (Madge and Barker 2007)"[7]

Allowing young people to develop an understanding of risk in both the real and virtual world is a crucial element of their personal development. As research by Ofcom shows, a majority of parents believe that the benefits of their child's technology use outweigh the potential harms,[8] and have a positive impact on their future, career, and life skills.[9]

There are also concerns around the difficulty of securing genuine parental consent without children providing false details to access online services. Child safety experts believe that requiring parental consent from all users under the age of 16 years would significantly increase the likelihood of teenage users lying about their age and accessing age-inappropriate services (designed for adults) rather than accessing versions of online services with age-gating and additional privacy settings which are designed to safeguard young people.

Theme 11 – Freedom of Expression in the Media

Articles 85 (1) and (2) refer to Member States taking steps to protect the freedom of expression and information, both of which are key in democratic societies. The Government must maintain the exemption set out in section 32 of the Data Protection Act 1998. techUK would further recommend that Government should consult, specifically with the ICO and industry, on the merits of further broadening the exemption. Government will be aware of the growing use of data protection law by influential claimant lawyers to bypass the stricter test of libel and other laws to secure the removal of content from online services and suppress legitimate speech, which may be in the public interest. Section 32 of the Data Protection Act provides a defence to the media publisher, but not online intermediaries on whose platforms publisher content may have been shared. This derogation is an opportunity to close the lacuna in the law, by maintaining the current exemption and extending it to intermediaries.

[7] https://www.iwf.org.uk/sites/default/files/inline-files/Safer%20Children%20in%20a%20Digital%20World%20report.pdf
[8] https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf
[9] https://www.fosi.org/policy-research/parents-privacy-technology-use/

Theme 12 – Processing of Data

Many of the articles covered in this theme refer to requirements under Member State law. The Government should set out what Member State laws may be involved, and consult with industry, to determine whether derogations are necessary.

Articles 6 (2), 6 (3) and 18 (2) all refer to similar derogations relating to the processing of data based on legal obligations and public interest. As mentioned in relation to Theme 6, clarification on what the Government's definition of public interest would be helpful, and consultation would be welcome.

Articles 88 (1) and (2) could be used to provide companies with clarity about what is and is not acceptable processing of personal data for employment purposes. The Government should consult with the ICO on its current employment practices code.

Theme 13 – Restrictions

Article 23 allows member states to legislate to restrict the application of various rights and duties under this regulation. By and large the Government should maintain existing exemptions under the Data Protection Act 1998, however not all will be appropriate to fit with the GDPR. **Where the Government is considering implementing restrictions under this derogation it should consult with industry to understand possible implications**. It is difficult to provide more detailed opinions on this derogation as the Government have not made public where they may be considering implementing restrictions under the Article 23 derogation.

Additional Question – cost impact

It is difficult to provide a response to this question as the cost impact on businesses is not yet fully understood. **The Government should produce an impact assessment to provide that understanding**. Once an Impact Assessment is published businesses will then be able to make suggestions as to how to minimise the cost.

ANNEX 1 - techUK's response to European Commission's 'Building a European Data Economy' Communication Consultation – Submitted 26 April 2017

Free Flow of Data

A modern digital economy and society cannot thrive without an open borderless world when it comes to data. Data-driven innovation is underpinned by the flow free of data across borders. That is why techUK supported the Commission's ambition to pursue legislative action to end unjustified data localisation restrictions that are a barrier to the free movement of data, and was disappointed when this did not happen[10.]

Existing national barriers, both direct and indirect, to the free flow of data are a concern for any business operating cross borders. Barriers to data flows undermines the ability of digital companies, particularly digital startups and scale-ups from across Europe, to grow and scale and for these businesses to benefit from the adoption of innovative digital technologies such as cloud computing, machine learning and AI. The reality of existing localisation requirements for start-ups and SMEs is the replication of business structures and processes in multiple Member States within the single market. This means that European startups are facing an often confusing patchwork of national laws that is an active disincentive for startups who look to build and scale their business in Europe and as a result could ultimately slow down the pace of digital transformation across Europe.

The Commission must remain resolute on this issue given the economic impact on data-driven start-ups of not removing existing inappropriate and misplaced data localisation requirements. A recent report estimated that data localisation policies raise the cost of hosting data by 30-60%[11.] This is money that could be spent on developing innovative digital products and services that could help to drive Europe's Digital Single Market forward.

As the Commission's impact assessment noted, the removal of data localisation restrictions would add an estimated 8 billion Euros per year to the European economy. This is not just an issue that impacts tech start-ups but all sectors of the European economy that stand to gain from Europe's transformation to a data-driven economy. If data localisation requirements are not addressed all business will face increased costs and a reduction in business agility, flexibility and competitiveness.

[10] https://www.techuk.org/insights/news/item/10028-free-flow-of-data-proposals-risk-stunting-europe-s-digital-growth
[11] http://www.itic.org/news-events/techwonk-blog/the-costs-of-data-localization

It is understood that a reason for the Commission not yet introducing regulation in this important area is that there may be a perception that data is more secure when it is stored locally. This perception is simply not correct. In fact, it is suggested that data stored in one geographical location without a secure backup of the data stored elsewhere could put data, and organisations operational effectiveness, more at risk. The industry has invested significantly in developing security tools and technologies that can be deployed to ensure data is stored and managed to an appropriate level of security wherever the data resides.

techUK would welcome proposals from the European Commission on what can be done to address such perceptions. It is suggested that the work conducted by DG Connect on promoting the security of the cloud computing market, for example the development of the European Cloud Scout[12] tool for SMEs, could be extended to consider and address data security perceptions.

We urge the Commission to move forward with a regulation to enshrine the free flow of data and remove unjustified data localisation restrictions and unlock the full economic and societal power of data.

[12] http://cloudscout.cloudwatchhub.eu/#/app/home?lang=en&code=en