Open Rights Group - Response to DCMS call for views on GDPR derogations

Open Rights Groups welcomes the opportunity to respond to this call for views. The General Data Protection Regulation (GDPR) sets out many new rights for UK citizens, including better notions of consent, transparency, the right to obtain and download our information.

However, many of the new rights will depend on enforcement. There are serious fines available when companies don't comply, which should make a big difference, but enforcement requires someone to take initial action. One of the better ideas in the regulation is to allow non-profit privacy groups to launch complaints without having to find specific individuals who have been directly affected, and to help people sue companies for compensation. The GDPR requires member states to choose to allow this, or not, and we very much believe this should be legislated for in the UK.

In the overall approach to derogations, we believe that Brexit should be an important consideration. The UK will require the EU to agree to let data flow without restrictions on the basis that UK law is as good as the EU's. GDPR greatly helps with this, but derogations that set the UK in a unique course risk pushing the UK data protection regime into incompatibility. This would be an economic disaster.

The exemptions in the Data Protection Act should not be expanded from those in the current DPA when implementing the GDPR; and as we discuss below, in many cases these will need to be reviewed in light of the more stringent requirements for legal certainty.

The new data protection regime under GDPR and beyond should be implemented by primary legislation in order to allow a full debate in Parliament that ensures the involvement of all stakeholders, including the organisations protecting the interests of citizens and consumers. This legislation should incorporate the Law Enforcement Data Protection Directive that complements the GDPR.

Any changes in the UK's implementation of the GDPR post Brexit should not be implemented by Great Repeal Act Henry VIII powers, as these will likely concern the rights of data subjects or the protection afforded to data subjects.

We advise against the temptation to fast track this legislation. We are already deeply concerned about the apparent lack of resources for this Call for Views, which sets out no background at all for the consultation, so only experts can practically respond.

Cabinet Office guidelines state that consultations should *"give enough information to ensure that those consulted understand the issues and can give informed responses."*[1]

We assume that the lack of detail on the government's analysis and approach to the derogations is the result of a severe lack of resources for key privacy laws like the GDPR. Ministers should be allocating more resources, or we will start to see serious policy mistakes being made.

This document relies heavily on the collective analysis of the exemptions in GDPR performed by the European civil society organisations Privacy International, Bits of Freedom, Panoptykon, FIPR, AccessNow, and EDRI, of which ORG is a member[2].

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492132/20160111_Consultation_principles_final.pdf

[2] https://edri.org/files/GDPR_analysis/EDRi_analysis_gdpr_flexibilities.pdf

Theme 1 - Supervisory Authority

Article 58 - Powers

The ICO should be able to recover the costs of an audit and enforcement if the data controller is found in breach of the GDPR. This will help the finances in the absence of compulsory registrations.

Theme 2 - Sanctions

Article 36 - Prior consultation

The provision makes “prior authorisations” an option in relation to risks around “the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health.” In practice, this will mainly apply to public bodies – but some “tasks” performed by private entities, such as fraud detection, can also be argued to be “in the public interest”.

We support the need for prior authorisation for certain high risk processing in the public interest. The Digital Economy Act 2017 creates vast new powers for ministers to share data and the state will undoubtedly increase its data processing in the near future, leading to potential abuses.

Theme 4 - Data Protection Officers

Article 37 - Designation of the data protection officer

Article 37(1) makes the appointment of a DPO compulsory for public bodies, but for private bodies only in certain limited cases, i.e., when they carry out “systematic monitoring of data subjects on a large scale” or when their “core activities” involve processing of sensitive data “on a large scale”. The latter tests (“large”, “core”, “systematic”) are already vague – and this requirement is therefore certain to be applied differently in the different member states (unless the cooperation-, mutual assistance- and consistency mechanisms are used to avoid that).

Secondly, it says that MSs may also extend this duty to other entities than those covered by Article 37(1), i.e., to private entities not carrying out “systematic monitoring of data subjects on a large scale” or processing of sensitive data “on a large scale”. This

is likely to be done in countries such as Germany that have a long history of requiring a DPO in most sizeable companies.

We see this as an opportunity to help companies improve their data handling and would support an approach where DPOs are appointed in many companies. We would be concerned that the UK may implement a very narrow interpretation of the rules, with only a small minority of companies investing in a DPO. Shared external DPO roles should be explored to make it more affordable.

Article 38 - Position of the data protection officer

This provision stipulates that secrecy and confidentiality requirements incumbent on DPOs can be determined by EU or MS law. This could be problematic with regard to exceptions to such duties, in particular in relation to compulsory disclosures of information to law enforcement and national security agencies.

The communications of a DPO would also need to be considered in the protections of certain communications - legal, journalistic, medical - from disclosure and surveillance.

Theme 5 - Archiving and Research

Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 9(2)(j) can lead to serious abuses of sensitive data for anything labelled “archiving in the public interest” or “scientific” uses, including use of such data for commercial research. The second and third paragraphs of Article 89 seriously aggravate this, by expressly allowing MSs to adopt different – more/less strict – rules in this regard, subject only to the very vague data minimisation / pseudonymisation / anonymization requirements of Article 89(1) (with minor variations between the permitted exemptions from data subject rights regarding archiving and scientific research).

Between them, these provisions create dangerous loopholes in the protection of personal, and especially sensitive, data. The permitted derogations from articles 15 and 16 would seem gratuitous and not relevant in most cases. Articles 18 and particularly 21 could admittedly impact research, but article 21 in particular already contains a

provision where subjects cannot object to research in the public interest, which we think should be the main principle here.

Theme 6 - Third Country Transfers

Article 49 - Derogations for specific situations

Article 49(1)(d) allows the transfer of personal data to third countries without adequate data protection, without the consent of the data subjects or any other basis for the transfer as listed in Article 46(1), if the transfer is “necessary for important reasons of public interest”; and para. (4) adds that the “public interest” in question must be “recognised in Union law or in the law of the Member State to which the controller is subject”.

Recital 112 lists as examples of relevant transfers: “international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or in order to reduce and/or eliminate doping in sport”; transfers which are “necessary to protect an interest which is essential for the data subject's or another person's vital interests”; and “transfer[s] to an international humanitarian organisation of personal data of a data subject who is physically or legally incapable of giving consent, with a view to accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed convicts”. However, these are only examples.

Presumably, all the special public interests listed in Article 23 could also qualify as such interests: national security, defence, public security, the prevention or investigation of crimes, “other important objectives of general public interests”, protection of judicial independence, breaches of professional ethics, protection of data subject rights, “a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority”, and even enforcement of civil law claims (the claims may be private, but the general principle of enforcement of civil claims serves a wider public interest: upholding the rule of law, also in transnational cases).

Some of these interests are already excessively broad and vague, which means that their application in practice is not foreseeable (which contravenes the rule of law in itself). But Article 49(1)(d) allows MSs to actually go even beyond those purposes: the “public interests” listed here are left completely undefined. It could include, for instance,

“maintaining good relations” with the third country to which the data are to be transferred, or even “boosting trade”.

As it stands, this provision is effectively a carte blanche handed to the MSs, allowing them to circumvent the otherwise seemingly strict rules on data transfers. The understanding of the public interest transpiring from the Regulation is dangerously close to the interests of the state or certain public bodies.The UK should not abuse this provision to hollow out data protection, and instead should define narrow exemptions and establish a public interest tests in law.

49 (1)(g)
This provision allows the transfer of personal data to third countries without adequate data protection, without the consent of the data subjects or any other basis for the transfer as listed in Article 49(1)(b)-(f), if the data come from “a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest”, provided that “the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.” This applies, e.g., to land, buildings or company ownership registers, access to which is typically granted by law either to everyone (registers open to the public) or to certain categories of people specified in the law regulating the register, e.g., house buyers or litigants.

In principle, this may seem unproblematic. However, the EU DPAs have made clear, in several “Article 29 Working Group” opinions,** that under EU data protection law, data released from public registers should remain subject to the purpose-limitation principle, and that the data once released can therefore not be used for any other purpose. It is notable that the provision refers to compliance with the conditions for “consultation” of the data – i.e., with the conditions for access to and obtaining of the data – but not to any conditions that may be imposed on the further use of the data.

When data from public registers are transferred to third countries without adequate (or indeed any) data protection, the WP29’s important limitation is very likely to be ignored. In other words, the provision is likely to lead to the loss of control over the use of data that can be obtained from public registers, or registers open to certain categories of people, in the EU, contrary to the purpose- limitation principle. For instance, in the USA, data that have been made public effectively lose all privacy protection.

Theme 7 - Sensitive personal data and exceptions

Article 9 - Processing of special categories of personal data

9(2)(a)

This provision allows MSs to prohibit, in certain contexts, the processing of so-called “sensitive data” (or some categories of sensitive data), even with the consent of the data subject. This is currently done in some MSs that, for instance, prohibit employers from asking for certain sensitive data from their employees: they are not allowed to collect and use such information even with the consent of the data subjects.

Current provisions in Schedule 3 of the DPA should be maintained.

9(2)(b)

This provisions allows MSs to require the (collection and further) processing of sensitive data under employment-, social security- or social protection law. There should be restrictions on the use of such sensitive data, especially by private entities or (public- or private sector) employers for purposes not directly related to the operation of the relevant employment-, social security- or social protection law.

These provisions are potentially broader than what is currently allowed in the DPA, particularly under “social protection law”. During the passage of the Digital Economy Bill 2016, civil servants expressed to us that data protection legislation would provide safeguards, but clearly we cannot rely on GDPR to restrict the uses of sensitive data in such context.

9 (2) (g)

The provision allows MSs to adopt laws authorising processing sensitive data for reasons of “substantial public interest” (without consent or any other legal basis). Recital (56) seems to legitimise the UK practice of political parties compiling regional and wider databases on the political allegiances of all households, without the consent of the data subjects; something that would be regarded as in manifest breach of data protection in other countries.

Given the current concerns about microtargeting in elections, these practices should be properly scrutinised.

9 (2)(h), 9 (2) (i), 9(4)

Article 9(2)(h) allows for MSs to provide for specific rules allowing the processing of data for very broadly-formulated health care and health-related purposes without consent, not only on the basis of a Union or MS law, but also “pursuant to contract with a health professional”. Although the article adds that this must be “subject to the conditions and safeguards referred to in paragraph 4”, these in fact only require the data to be “processed by or under the responsibility of a professional subject to the obligation of professional secrecy” or “by another person also subject to an obligation of secrecy”. The details are to be spelled out in national law or in “rules established by national competent bodies”.

This is a highly contentious area and we expect DCMS to spell out in detail any proposed changes.

9 (2)(j) & 89
Member states can authorise the processing of sensitive data without consent for archiving purposes done in the public interest, or for historic and scientific research, subject to the requirements of Article 89(1). The latter, however, mainly only reiterates the (in any case applicable) requirement of data minimisation and maximum pseudonymisation or (where possible) anonymisation of data held for historical/archival/scientific purposes. “Public interest” is not defined and the scope of this provision is consequently essentially left to the MSs (which in practice can be heavily affected by temporary political priorities).

There is a risk that private- and public-sector research bodies (which are increasingly intertwined) will try to stretch the provision to allow them to do anything they want with sensitive data they can obtain, certainly also for commercial “research” purposes.

9 (4)
This provision stipulates that MSs “may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or health data”. It should be made clear (e.g., by the EDPB) that this wording does not allow MSs to relax the rules in the GDPR further than as expressly envisaged in the Regulation: they can impose conditions that do not amount to limitations (e.g., purely technical standards), or conditions that do amount to limitations, but not conditions that amount to relaxations of the rules. Even then, this provision is problematic in any transnational/online context.

Theme 9 - Rights and Remedies

Article 17 Right to erasure ('right to be forgotten')

The provisions allow the EU and the MSs to lay down “legal obligations” requiring (certain) data to be erased in certain circumstances. In relation to the RTBF, this means that that right can also be used by data subjects to enforce adherence with such legal obligations, irrespective of other reasons to exercise the right. This appears to be the case right now.

We are unsure however how current ICO guidance on data deletion may operate with these explicit rights to erasure. In the context of current DPA requirements that data is not held longer than necessary, the ICO is satisfied that information has been ‘put beyond use’, but not actually deleted[3]. We expect that these guidelines may need to be reviewed.

The right to be forgotten in particular should be implemented in a way that shows it is an equal balance between privacy and freedom of expression, as this will defuse the misunderstanding of the provision.

Article 22 (2)(b) - Automated individual decision-making, including profiling

The provision enables member states to adopt laws authorising fully-automated decisions and profiling (note: by private - and public sector controllers) that produce legal effects for the data subjects or otherwise “significantly affect” them, outside (pre-)contractual contexts and without the consent of the data subject. Such “legally authorised” decisions and profiles must be subject to “suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests”.

However, different from automated decisions and profiling in (pre-)contractual contexts or with the consent of the data subject, for “legally authorised” decisions and profiles, these need not include “the right to obtain human intervention on the part of the controller, to express his or her [i.e., the data subject’s] point of view and to contest the decision” (cf. Article 22(3)). It is difficult to see what kinds of safeguards other than “human intervention” and a right of data subjects to contest a fully- automated decision can ever be as effective or therefore “suitable”.

Nevertheless Article 22(2)b requires that Member State law authorising profiling contains safeguards. We are concerned that legislation such as the Digital Economy Act 2017 that enable data processing that will lead to automated profiling do not contain

[3] https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf

such safeguards. If codes of practice are to provide that law-making function they need to be fully enforceable and specifically address profiling.

The ICO has called for feedback on automated profiling[4], as its "stakeholders have identified profiling as an area of concern and the Article 29 Working Party (WP29) has prioritised it for guidance". Once that guidance has been issued we would expect that any relevant legislation will follow it in setting up suitable safeguards.

Article 26 - Joint controllers

When processing is carried out by several "joint controllers" acting together, this provision in principle leaves it to those controllers to determine their respective roles and compliance responsibilities between them in what is called an "arrangement between them". There is no requirement that this arrangement be put in writing, or be submitted to the ICO (although presumably, in any inquiry, the ICO can ask for the details of the arrangement to be explained to them).

There are only a few requirements for such an arrangement. It must "reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects", i.e., at least in relation to the data subjects it must reflect actual divisions of power, control and responsibility: the arrangement should not be a deceptive front hiding the real divisions of responsibility. However, it will be difficult for data subjects to gauge this since, under this provision, they are only entitled to be provided with "the essence" (i.e. not the detail) of the arrangement, on request. The only sop provided to the data subjects is that they can exercise their rights under the Regulation "in respect of and against each of the [joint] controllers." The latter "may" moreover "designate a [presumably single] point of contact for data subjects" – but even that is not required.

This provision grants excessive freedom to joint controllers – which are increasingly common in the increasingly complex chains of companies involved in commercial activities, in particular also online – to choose "arrangements" for themselves that place their operations under the (for them) least demanding regime. We expect disparities across Europe in this respect that could lead to jurisdiction hopping. Corporations will try to benefit from the lax rules and avoid the strict ones; and this provision gives them a means to try and do so.

In order to counter this serious risk, the stipulation that the "arrangements" should reflect actual divisions of responsibility rather than create evasions from strict rules in some MSs, should be strongly and firmly enforced by the ICO, also and in particular in relation to multinational corporations, and/or corporate chains operating in the online environment, especially by means of the cooperation-, mutual assistance- and consistency mechanisms in the Regulation.

[4] https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf

Article 80 - representation of data subjects

The GDPR introduces the possibility for non-profit privacy organisations to take a much more prominent role in the representation of data subjects by enabling these groups to lodge complaints independently of a data subject's mandate and to receive compensation on their behalf. These provisions are some of the most important changes towards effective protection introduced in the Regulation and are the main priority for civil society.

The mandatory provisions allowing data subjects to mandate a privacy group to help exercise their rights is useful but unfortunately not enough. We expect the UK to implement these optional provisions, and would interpret a refusal as a deliberate attempt to reduce effective data protection for people in the UK.

Citizens face increasingly complex data ecosystems in environments such as the Internet of Things, online behavioural advertising or political microtargeting. Personal information flows across myriad organisations and it is transformed - in some cases identifiers are removed and then at a later stage the data is relinked to identifiable information. It is almost impossible for an average person to be able to know which organisations hold their personal data.

Privacy groups can carry out research and are able to track who may be processing the data and at what point breaches may occur, but it may well be impossible for these organisations to contact any of the affected subjects to inform them of the problem and encourage them to mandate the group to take action.

In many cases these data ecosystems are so opaque that we rely on whistleblowers to explain abuses that would remain completely hidden from the public and any affected individuals.

Enabling privacy groups to take independent action will increase the effectiveness of enforcement and help the ICO focus its resources better, as privacy groups will have to carry out initial investigations and perform due diligence before launching a complaint.

We cannot see any downsides to enabling these optional provisions. There are already similar provisions in the UK for "super-complaints" raised by organisations

independently of affected individuals in finance and consumer protection[5]. There are clear criteria for the designation of those allowed to lodge super-complaints[6]. Given the strict criteria set out in the Regulation - non-profit, public interest and active in data protection - we believe that a fairly small number of organisations will qualify. Any “ambulance chasers” will clearly be excluded.

The mandatory ability for certain privacy groups to help data subjects pursue Article 79 claims in court against a controller will be a critical aspect in ensuring effective access to remedies that ensure citizens trust the data protection framework. For this to happen, we believe the UK must also implement the optional provisions in Article 80(1) allowing privacy groups to help exercise the right to receive compensation under Article 82.

We also believe that a small proportion - e.g. 10% - of fine revenues should be channelled to support privacy organisations that can satisfy public sector audit requirements for public money with activities - including public education and legal action - that aim to protect the position of data subjects under the GDPR. The ICO mainly works with organisations and it will be harder and more expensive for them to reach out directly to individuals in an effective manner.

Theme 10 - Processing of Children’s Personal Data by Online Services

Article 8 authorises the MSs to set the age of children's consent to the signing up to information society services anywhere between 13 and 16. This provision introduces specific protections for children restricting their ability to consent to data collection and processing without parental authorisation under a certain age. In case of children, the GDPR fails to shift the balance of rights back towards the individual and leaves children’s rights seriously flawed.

The consent-based model specified in the GDPR is not compatible with the nature of web content. Even children who are not particularly tech savvy will be able to bypass parental consent by creating a bogus email address for their “parents”. This also raises further questions of whether parents are aware of their children’s data being collected and whether they themselves understand the consequences of data collection.

[5] https://www.gov.uk/government/publications/what-are-super-complaints/what-are-super-complaints

[6] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200454/guidance_for_super_complainants_120313.pdf

The current UK law does not provide a definition of a child based on age. The threshold for parental consent is non-obligatory age of 12. The ICO guidance[7] suggests that both the age of a child and assessment of their maturity should be the decisive factors in children's data processing. Only in very specific sensitive cases the ICO expects data controllers to obtain parental consent for children over the age of 12.

ORG supports this hybrid model for processing children's data. The upper age limit of 16 years as specified in the GDPR will cut children of from the Internet and access to legitimate information. This can have serious impacts on their freedom of speech.

We believe that balance between children's consumer protection and their right to participate online could be struck more effectively by placing more importance on children's understanding of data processing. Therefore it is crucial that they can access this information in a children appropriate format.

We recommend the Department conducts further consultation on this issue. No account has been taken of evidence or views from children and young people themselves before the age consent limits were proposed in the GDPR.[8] Further policy research on age limits is soon to be available[9] in the public domain and should be taken into account when deciding on restricting children's ability to consent to data collection and processing without parental authorisation.

We encourage the Information Commissioner and government to take a forward-thinking, considered and evidence-based approach to laws on the age of consent and age verification, with academic, civil society and ICT stakeholders input. This will ensure that thorough consideration is given to participation rights as well as protections policy and legislation.

This policy should be backed by a collective action from policymakers and legislators, developers, providers and product suppliers, in order to enable enforcement and educating the public.

---

[7] https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf

[8] http://defenddigitalme.com/2017/03/gdpr-compliance-and-children/

[9] http://blogs.lse.ac.uk/mediapolicyproject/2016/10/17/to-be-13-or-16-that-is-the-question-the-implications-for-uk-teenagers-of-the-european-general-data-protection-regulation/

Theme 11 - Freedom of Expression in the Media

Article 85 - Processing and freedom of expression and information

Article 85(1) stipulates that MSs must reconcile in domestic law the right to data protection and freedom of expression. This includes exemptions or derogations from the basic data protection principles, the rights of data subjects, the duties of controllers and processors, restrictions on transborder data ows, the supervision by DPAs, “if they [i.e., such exemptions or derogations] are necessary to reconcile the right to the protection of personal data with the freedom of expression and information.”(85(2))

Article 85 repeats broadly similar general derogations that were already introduced under the Data Protection Directive. Currently in the UK journalistic uses of personal information can be exempt, if publication is in the public interest and compliance would be incompatible with journalism. The journalism exemption in the UK can exempt the media from the data protection principles and removes the right to access, prevent processing, rectification, blocking and erasure, in appropriate cases - but never principle 7 (security) or the section 55 offence. The ICO expects media organisations to be able to explain why the exemption is required in each case, and how and by whom this was considered at the time. Justifying public interest heavily relies on the reasonable belief of the data controller. The government must explain whether it will maintain its current approach and what legal instrument will be used.

The Regulation is potentially broader in scope than the current Directive, “including [but not limited to] processing for journalistic purposes and the purposes of academic, artistic or literary expression”. In the digital age, it is increasingly difficult to define “journalistic, academic, artistic and literary” activities. Many people publish, express themselves or post their opinions online, often to a wide audience. Recital 153 rightly says that “In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly”.

The UK DPA does not define journalism, but the ICO guidance[10] says that this exemption can apply to online bloggers who are not journalists or non-media organisations. Their guidance allows for a very wide public interest justification but

[10]https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

specifies that DPA mandates identity protection of individual sources. This will need to be further clarified in UK law.

The second paragraph of Article 85 gives no guidance whatsoever on the precise scope of the exemptions that might be "necessary". In some respects – e.g., as concerns the principle that processing should be "fair and lawful", or as concerns the requirement that "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" – it is difficult to see how any exemption could ever be necessary. At the very least, we expect that the new European Data Protection Board will issue guidelines urgently on how this provision is to be applied; and we hope the UK government will consult civil society, including freedom of expression and digital rights groups before setting this exemption in domestic law and notifying the EU.

The term "necessary" refers to Article 52(1) of the Charter, which means that the laws adopted (or retained) by the MSs in this regard can, when they touch on privacy and data protection, be tested on that "necessity" - and on their clarity and foreseeability, etc.- in the courts, including the CJEU. In the context of Brexit, we will need to understand what substitutes the Charter in providing the fundamental rights basis and how the UK Supreme Court will work with European courts in international cases.

Theme 12 - Processing of Data

Article 6 Lawfulness of processing

Tasks carried out in the public interest, with official authority or for legal obligations have to be based on law in sufficient detail. It is difficult to see how this requirement can work with the "permissive power" approach favoured by government to create data sharing powers in the public sector. We believe that this will require a review of many existing data processing practices and the expectations of widespread intragovernmental data sharing enabled by the Digital Economy Act 2017.

Article 35(10) - Data protection impact assessment

This provision relates to the situation in which processing is carried out in compliance with a legal obligation, in the performing of a task in the public interest, or in the exercise of public authority (Article 6(1)(c) & (e), above) and is based on EU or MS law. In such cases, if the relevant law regulates the specific processing operation or set of operations, and a DPIA has already been carried out for that operation or set of operations as part of a general impact assessment carried out in the context of the

adoption of the relevant law, a new DPIA of any new processing operation of the same kind is not required.

This appears to be unproblematic, provided the original (general) DPIA was thorough; the new operation is indeed of precisely the same kind as was assessed in that original DPIA; and the legal rules and interpretations of the rules or technical or ethical standards in question have not changed.

We are concerned, however, that this provision could be easily abused to avoid the kind of scrutiny that a DPIA is meant to provide, and will expect clear guidelines on when a new assessment is required. For example, the Digital Economy Act 2017 enables very dynamic data processing in the public sector with new types of data and analytics being constantly deployed to tackle social welfare, fraud and debt. The original DPIAs will quickly become obsolete.

Article 87 - Processing of the national identification number

It was already recognised in the 1995 Directive that national identification numbers and similar identifiers of general application – such as the UK national insurance number, NHS register number or Scottish Unique Citizen Reference Number, used in a number of systems including the Scottish Entitlement Card and myaccount system[11] – pose risks in terms of data protection. Article 87 also recognises this and again leaves this up to the Member State to regulate. However, it now requires that the numbers are "used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation."

UK provisions for general identifiers in the DPA have not been clearly applied and the GDPR provides an opportunity for clarification on when these should be used and what are appropriate safeguards, particularly on the use of the National Insurance Number (NiNo)[12]. We think that this is the moment to identify and regulate other internal identifiers of general application used to match datasets in the public sector.

[11] http://www.entitlementcard.org.uk/sites/default/files/TermsandConditions.pdf and see https://scotland.openrightsgroup.org/policy/2015/02/02/a-national-id-system-by-the-backdoor:-thenhscr-scotland-consultation/

[12] https://www.theregister.co.uk/2015/12/22/national_insurance_number_consent_dwp_say_wider_nino_use_is_no_longer_a_nono/

Theme 13 - Restrictions

Article 23 - Restrictions

The article authorises member states to restrict by law the application of data subject's rights for purposes of national security, defence, public security, the prevention or investigation of crimes, “other important objectives of general public interests”, protection of judicial independence, breaches of professional ethics, protection of data subject rights, “a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority”, or enforcement of civil law claims. Apart from the addition of the last issue (civil claims), the provision is largely the same as the corresponding one in the 1995 Data Protection Directive (Article 13(1)), but expands on some important conditions, i.e., by stipulating that each such legal restriction must “respect the essence of the fundamental rights and freedoms” and must be “a necessary and proportionate measure in a democratic society” to safeguard the listed interests. It also usefully adds that the law in question must contain “specific provisions” setting out the purposes of the processing, the categories of data concerned, the scope of the restrictions, the rights of data subjects (limited though these may be) and the relevant safeguards “to prevent abuse or unlawful access or transfer” (Article 23(2)).

This higher bar of legal compliance may render the some of the exemption practices in the UK wanting, such as the national security certificates under Section 28 of the DPA. We believe that these certificates should be subjected to independent judicial authorisation along the lines of the Investigatory Powers Act 2016.

We would recommend a full detailed review of the exemption/restrictions regime to ensure compliance with GDPR, as compliance with the conditions just mentioned is now a matter of EU law: MSs can be challenged for non- compliance with these conditions – e.g., on the basis that an exemption is too broad, or that the applicable safeguards are ineffective – and the matter can ultimately be determined by the courts.