BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Call for views on the General Data Protection Regulation derogations - Big Brother Watch Response

May 2017

About Big Brother Watch
Big Brother Watch is a civil liberties and privacy campaign group that was founded in 2009. We have produced unique research exposing the erosion of civil liberties in the UK, looking at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this process Big Brother Watch has produced a number of reports looking at standards of data protection across the public sector. We have also campaigned for individuals to be given more control over their personal data.

Overview
Our society is driven by data. The time where digital engagement was a choice is fast coming to an end. Increasingly online engagement and the sharing of personal information is becoming a necessity. This change will alter how we consider and engage with our personal data, particularly in relation to the level of control and data ownership we are entitled to.

Big Brother Watch is supportive of the General Data Protection Regulation (GDPR) and welcomes the UK Government's intention to implement the Regulation in May 2018.

The correct implementation of the GDPR will have a huge impact on whether or not the UK will be able to successfully gain an adequacy ruling once it leaves the European Union. Failure to gain adequacy will have severe consequences, however this is an issue which is outside of the scope of the consultation, for this reason our response will be limited to the process of applying the GDPR to UK law. However we would like to see further scrutiny of the adequacy issue over coming months from the Government.

Response

THEME 2 - SANCTIONS

Article 36 – Prior consultation
We support the concept of prior consultation and the use data protection impact assessments in order to determine the level of risk in the processing of data.

We believe it is right that the relevant authority; namely the Information Commissioner, will be able to request further consultation with the data controller to ensure that the points outlined in Article 36(3) (a) to (f) have been considered.

We see this as a positive step which will improve transparency and ensure proper consideration of the nature, purpose and method of the processing.

We would like to see the requirement be undertaken for all data sharing within government. We say this in response to the many of the problems highlighted by the National Audit Office in their 2016 report "*Protecting information across government*"[1].

It is clear that there are profound problems across government with data protection and data breach relating to a lack of understanding of what the risks may be, poor training and a misinterpretation across departments of the Data Protection Act. These problem areas were reemphasised during the oral evidence[2] given to the Public Accounts Committee in their scrutiny of the NAO report the two witnesses, Paddy McGuiness, Deputy National Security Adviser, Intelligence Security and Resilience and Ben Aung, Deputy Director, Cyber and Government Security Secretariat, who outlined that many government departments believe they understand how data breach reporting works and yet in reality revealed that there is vast disparity across departments when it actually comes to collecting breach data and reporting breaches.

Article 36, if applied to all government departments sharing personal data, would arguably help data controllers within these departments fully understand the impact of any data they process and the negative consequences of a breach. This would we believe serve to improve standards so that the multitude of problems outlined by the NAO and during the evidence to the PAC do not persist.

Article 58 – Powers
We support the introduction of Article 58 in its entirety. Without the ability to investigate wrongdoing, issue corrective notices and provide guidance and advice no supervisory authority would be able to function effectively. Any watering down of the powers outlined in this Article would be unacceptable.

Should any additional powers such as those suggested in paragraph 6 be considered necessary, they must be published for wider public scrutiny ahead of any parliamentary debate.

Article 83 – General conditions for imposing administrative fines.
We welcome the financial fines mentioned in Article 83(4) and Article 83(6). We believe the figures outlined will play a critical role in deterring many data controllers from adopting poor data protection practices. However we do not believe that these fines will be a strong enough deterrent for all data controllers; to address this issue we will continue to argue for the introduction of custodial sentences, something we believe will act as a far greater deterrent.

Our primary concern with Article 83 is paragraph 7, the wording of which appears to indicate that despite outlining what the fines should be Member States will have the opportunity to determine their own fines for public bodies. Were this derogation adopted it would establish a clear and potentially contentious disparity within Member States between punishment for public and private sector organisations. Any change also risks causing confusion between Member States as fines for the same behaviour would vary between jurisdictions.

Looking specifically at the UK, we would recommend the Government adhere to the fines set by the legislation rather than try to decrease them.

---

[1] https://www.nao.org.uk/wp-content/uploads/2016/09/Protecting-information-across-government.pdf
[2] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/public-accounts-committee/protecting-information-across-government/oral/43227.pdf

Article 84 – Penalties
Should the UK seek to lay down rules on other penalties, we would recommend they look at the wide range of support for introducing custodial sentences to punish the most serious data breaches under Section 55 of the current DPA.

THEME 4 – DATA PROTECTION OFFICERS

Article 4 – Definitions
We have specific concern in relation to the latter part of paragraph 9:

"*public authorities may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.*"

It is not clear what *"a particular inquiry"* refers to. Without clarity, mistakes, misunderstandings and errors can occur which in the area of personal data can have profound consequences. We refer once again to the litany of problems outlined by the NAO in the 2016 report *"Protecting information across government"* as a clear living example of how misunderstanding and a lack of training and resources within public authorities has led to huge data protection problems.

Furthermore it is critical to note that in the UK public authorities have a patchy history when it comes to data protection. Reports published by Big Brother Watch have revealed the extent of data breaches by local authorities[3], the NHS[4] and the police[5] which give a clear indication of the problems faced by public authorities in the management and protection of data. Without clarity of definitions there is the possibility therefore that some public authorities may use the vagueness of language as a loophole to access, use, share or copy personal data, thereby sidestepping the protections required of those defined in the GDPR as "*recipients*".

Further detail explaining and outlining clearly what the UK Government define as *"a particular inquiry*" would minimise the potential for confusion.

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.
The derogations contained in Article 89 will restrict individuals from having direct engagement with their data and their ability to control how it is used.

---

[3] https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/08/A-Breach-of-Trust.pdf
https://bigbrotherwatch.org.uk/la-data-loss.pdf
[4] https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/11/NHS-Data-Breaches-Report.pdf
https://www.bigbrotherwatch.org.uk/wp-content/uploads/2011/10/NHS-Breaches-of-Data-Protection.pdf
[5] https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/07/Safe-in-Police-Hands.pdf

We support the idea of *"data minimisation"* outlined in paragraph 1, we also strongly support the intention that data shared or accessed for research purposes must not permit the *"identification of data subjects".* We raise concern however that anonymisation or pseudonymisation may be seen to be fail safe solutions for re-identification. Sadly they are not. Both techniques can enable re-identification if cross referenced with other data and it is vital that any data controller not only understands that but makes clear to any individual sharing personal data that there is a risk that re-identification may occur if the controller intends to cross reference now or in the future.

The processing and archiving of non-identifiable personal data by public bodies when it is for a clearly specified objective provides for some clear guidance to the individual but the opportunity within paragraph 2 and paragraph 3 to steer away from protections which are provided by Articles 15, 16, 18, 19 and 21 is a concern.

Our concern is specifically focused around the lack of definition for the term *"public interest"* in relation to scientific research, historical research or for a statistical purpose.

Without clarity and clearly set out guidelines it is more than possible that organisations will claim "*public interest"* when little evidence of public interest exists in order to either restrict an individual's access to their personal data or prevent the individual from having any further control over how their data is used.

We are concerned that the restriction of an individual's right to know what is happening to their data could be excused by public bodies for a range of reasons including to improve public wellbeing or societal improvement. This is particularly important in circumstances where an individual can be easily re-identified by the cross referencing or *"coupling"* of data.

We raise this in relation to the recent debate about Part 5 of the Digital Economy Act which revealed a strong desire within Government to keep the citizen at arm's length from their data. This approach is not forward looking and fails to acknowledge that citizens are increasingly digital by default and are required to be far more engaged with their personal data than ever before. Protection of data by the individual therefore is as time goes on instinctively going to become a daily matter of personal security. Attempts to restrict an individual's ability to see, control, consent or retract access to their personal data will cause unforeseen problems and could lead to a wide range of unintended consequences.

THEME 7 – SENSITIVE PERSONAL DATA AND EXCEPTIONS

Article 9 – Processing of special categories of personal data
As with other elements of the GDPR already referred to, Article 9 needs to establish clear definitions in paragraph 2(d) of what is meant by *"appropriate safeguards"* and in paragraph 2(g) and 2(j) as to what is meant by *"public interest"*. We trust that any definition of *"public interest"* would not include commercial activity.

THEME 9 – RIGHTS AND REMEDIES

Article 22 – Automated individual decision-making, including profiling.
We are profoundly concerned by the derogations outlined in paragraph 2 of Article 22 and the impact paragraph 2(a) and 2(b) could have on the individual in particular.

Profiling can be undertaken without an individual's knowledge. Profiling can involve the creation of a very detailed picture of an individual, their life, networks, routines, behaviour and history to name but a few.

We know that the use of profiling is prevalent amongst private companies and is used for marketing purposes, to determine amongst other things, people's moods, desires, concerns, attitudes, politics, religion, networks etc. We know that this data can be sold to or shared with a broad range of interested parties often invisible and unknown to the individual for purposes which the individual may object to.

Profiling with the intention of building broad range algorithms or to establish an automated decision making process can lead to inaccurate assessment of an individual which could potentially lead to a biased profile being created. For example, profiling of an individual based on their shopping habits may highlight a regular purchase of a large quantity of alcohol from a supermarket. The assumption based on the profile may lead a decision maker to assume that that individual has an alcohol related problem. This data could be shared with a GP, health care provider, health insurance provider, employer, DVLA etc. all of which has the potential to lead to a negative outcome for the individual despite the fact that they are teetotal but host a weekly book club where they provide alcohol for their guests.

Based on these derogations people will be unaware of what is being done with their data and will be given no opportunity to challenge decisions made or to seek redress for the impact errors may cause.

The UK should avoid seeking to make public or private profiling of individuals legitimate in order to establish an automated decision in relation to a contract or to public policy; even if it is perceived that the process would benefit the wellbeing of the individual or of society as a whole.

The intention of Article 22 paragraph 1 is excellent and we wholeheartedly support it. The intention behind the derogations in paragraphs 2, 3 and 4 however undermine the protection outlined in paragraph 1.

Article 26 – Joint controllers

Confusion about third party access to data is rarely made clearer after reading terms and conditions or privacy policies. Much of this confusion stems from the presence of unnamed or undeclared third parties which process personal data without the knowledge of the people the information relates to.

Article 26 does little to counter these concerns, appearing to overlook the need for far greater transparency in relation to whom a third party – or *"joint controller"* is.

We would recommend that any controller who is seeking to be a *"joint controller"* is required to provide their name, contact details, a description of what categories of data they will be accessing, for what purpose, for how long, where data will be stored and what technical and security measures will be used.

Furthermore we would expect to see a privacy notice outline the responsibilities which each of the controllers are to adhere to, this would ensure that the requirement for a *"transparent manner"* outlined in paragraph 1 is adhered to.

Article 80 – Representation of data subjects
We support the notion that the individual can seek independent guidance, advice and support from a not for profit body, organisation or association.

Individuals should be better integrated in the decision making process around what happens to their data. To ensure the success of any schemes of this kind, citizens must give their informed consent before any sharing takes place, unwanted access must be restricted and citizens must be made aware of how their data is being used. A key part of this process is ensuring that the citizen knows they can seek access to their personal data and have the right to seek redress should their data be misused, breached, stolen or hacked.

We recommend that individuals seek independent guidance from bodies, organisations and associations which have some legal skills and not solely because they are "*in the field of protection of data subject's rights and freedoms*" as outlined in paragraph 1.

THEME 12 – PROCESSING OF DATA

Article 6 – Lawfulness of processing
As with other Articles we would like to see clear definitions in relation to: paragraph 1(e) "*public interest*" and paragraph 1(f) "*legitimate interests*".

Paragraph 4 is of concern as it leaves decision making solely to the controller. As this paragraph deals with data which may relate to extremely serious issues such as national security, criminality and public safety a double lock process should be in place. We would envisage a new independent body being created to fulfil the second part of this lock. This would avoid the need to restructure the ICO and leave it free to provide effective external oversight of the functioning of the double lock process.

The combination of a proper double lock system and strong oversight from the ICO should ensure the transparency of decisions for further processing. This arrangement would also prevent the misuse or abuse of data as well as breaches of privacy and data protection in these sensitive areas.

Article 29 – Processing under the authority of the controller or processor
As with Article 28, this Article effectively unravels any of the protections citizens are entitled to in the rest of the GDPR if the processor is ordered to adhere to a Member State law.

THEME 13 – RESTRICTIONS

Article 23 – Restrictions
We acknowledge that if deemed to be "*necessary and proportionate*" protections will be removed by law enforcement and intelligence agencies for the purposes outlined in paragraph 1(a) to (j), however we query what the differences of definition are between "*national security*", "*defence*" and "*public security*".

We also raise concern that the provision laid out in paragraph 2(h) does not apply to UK citizens in relation to the Investigatory Powers Act 2016 (IPA). Despite challenge the Act provides no opportunity for citizens who have been subjected to surveillance and subsequently been found at the end of the investigation to be innocent of any wrongdoing, the right to be notified of the restrictions which have been placed on them and the opportunity to seek redress. We therefore query whether the IPA will cause issue with the UK's adherence to Article 23.