House of Commons

House of Lords

Joint Committee on Human Rights

The Right to Privacy (Article 8) and the Digital Revolution: Government Response to the Committee's Third Report of Session 2019

First Special Report of Session 2019–21

Ordered by the House of Commons
to be printed 29 April 2020

HC 313
Published on 1 May 2020
by authority of the House of Commons
and the House of Lords

Joint Committee on Human Rights

The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders.

The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

Current membership

House of Commons

Ms Harriet Harman QC MP (*Labour, Camberwell and Peckham*) (Chair)

Fiona Bruce MP (*Conservative, Congleton*)

Ms Karen Buck MP (*Labour, Westminster North*)

Joanna Cherry QC MP (*Scottish National Party, Edinburgh South West*)

Mrs Pauline Latham MP (*Conservative, Mid Derbyshire*)

Dean Russell MP (*Conservative, Watford*)

House of Lords

Lord Brabazon of Tara (*Conservative*)

Lord Dubs (*Labour*)

Baroness Ludford (*Liberal Democrat*)

Baroness Massey of Darwen (*Labour*)

Lord Singh of Wimbledon (*Crossbench*)

Lord Trimble (*Conservative*)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publication

Committee reports are published on the Committee's website at www.committees.parliament.uk/committee/93/human-rights-joint-committee by Order of the two Houses.

Committee staff

The current staff of the Committee are Miguel Boo Fraga (Senior Committee Assistant), Samantha Granger (Deputy Counsel), Shabana Gulma (Specialist Assistant), Zoe Grunewald (Media Officer), Katherine Hill (Committee Specialist), Eleanor Hourigan (Counsel), Lucinda Maer (Commons Clerk), and George Webber (Lords Clerk).

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on Human Rights, Committee Office, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 2467; the Committee's email address is jchr@parliament.uk

You can follow the Committee on Twitter using @HumanRightsCtte

First Special Report

The Joint Committee on Human Rights published its Third Report of Session 2019, The Right to Privacy (Article 8) and the Digital Revolution (HC 122/HL Paper 14) on 3 November 2019. The Government's response was received on 15 April 2020 and is appended to this report.

Appendix: Government Response

Introduction

The Government thanks the Committee for their report and the conclusions and recommendations it presents. We are committed to ensuring the UK maintains a high standard of data protection which protects the rights and privacy of individuals. At the same time, we want the UK to remain at the forefront of technological innovation because we believe that, harnessed properly, digital technology is an immense force for good.

As the Committee set out in their report, the internet has the potential to enhance our lives by supporting freedom of expression, the right to education, freedom of association and participation in elections. There are of course broader social benefits too. These technologies, if developed responsibly, can help transform public services and the relationship between governments and citizens. They can help us tackle some of the world's greatest challenges. For example, artificial intelligence is being used to detect breast cancer more accurately, predict areas at risk of flooding and identify sites where modern slavery is taking place.

We acknowledge the Committee's concerns that the widespread adoption of digital technology also poses new threats. If we cannot be confident that digital technologies are safe and secure, this may discourage their use. That is why our Online Harms White Paper set out plans for a new statutory duty of care, overseen by an independent regulator. The security of our digital platforms is also essential so that businesses and their customers are confident their money and data are secure. Through our National Cyber Security Strategy we are investing £1.9 billion to protect the nation online. We are also developing a new public cyber security campaign, planned to launch later this year, which will provide guidance on the proactive steps anyone can take to protect themselves against cyber attacks.

Regulations which are carefully designed and implemented can protect people and businesses from harm, whilst driving growth and innovation in the digital economy. Our data protection legislation was updated less than two years ago through the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulation (GDPR). It places stricter obligations on data controllers and processors to keep personal data secure. It requires organisations to make sure that it is processed where there are lawful grounds to do so and in a way that individuals would expect. It strengthens individuals' rights to seek to access, erase or rectify their data or to object to its processing. It also maintained the Information Commissioner as the UK's independent data protection regulator and modernised her investigatory powers and enforcement tools.

We do not share the Committee's view, as expressed in paragraph 32 of its report, that the existing legal framework does not provide enough protection against the misuse of people's data. As outlined below in response to the Committee's specific recommendations, this legislation should be capable of dealing with many of the issues outlined in the Committee's report, but it has not yet been fully tested. We will continue to keep the legislation under review as individuals and organisations become more familiar with it and as the Commissioner makes use of her new powers to tackle organisations which do not comply.

In addition to the new data protection legislation, the Centre for Data Ethics and Innovation has been established to look at complex emerging policy issues such as facial recognition technology, deep fakes and bias in algorithms. In the coming months, we will also be working with online advertisers to foster fair, transparent and ethical online advertising; and developing our National Data Strategy, so we can fully and responsibly unlock the power of data, for people and organisations across the UK.

More detailed answers to the Committee's specific conclusions and recommendations are included below.

Consent

1. **We consider that the vast majority of individuals would find it almost impossible to know what they are consenting to when using social media platforms or other web services. Individuals are highly unlikely to read or fully understand complex and lengthy terms and conditions or privacy notices. Moreover, these notices are non negotiable and offered in a take it-or-leave-it manner. Facebook, Snapchat, YouTube and many other online services make joining a service conditional on agreeing wholesale to terms and conditions, which includes current privacy notices and future changes to terms. In practice, this means individuals often have no choicebut to agree if they want to use a service, which raises questions about whether or not consent has really been given. (Paragraph 25)**

2. **Our view, based on the evidence we heard, is that the consent model is broken. It puts too much onus on the individual to educate themselves on how the technology companies work rather than setting a high standard of protection by default. (Paragraph 26)**

11. **Using the internet is an essential part of most people's day-to-day lives. But use of many websites and services is contingent on consenting to personal data being shared. This puts people's right to privacy at risk. It is likely that many people are unaware that they have agreed for their data to be shared, especially given the complexity of consent agreements. (Paragraph 49)**

The Government shares the Committee's concern about web services which make it difficult for users to understand how their data will be used and with whom it is going to be shared. Unless web services take their fairness and transparency obligations seriously, it is difficult for service users to provide properly informed consent for their data to be processed.

Article 5 of the GDPR makes controllers responsible for ensuring that personal data is processed fairly and transparently. When collecting personal data from individuals, the controller must provide them with information about the controller, the purposes for processing their personal data, and any third party with whom they intend to share the data. The GDPR is clear that data controllers must provide this information in a concise, transparent, intelligible, and easily accessible form, using clear and plain language. It places particular emphasis on the quality of communication with children.

In the Government's view, it is too early to conclude that online services cannot or will not comply with fairness requirements of the GDPR, nor that ordinary members of the public are incapable of making informed choices. Many websites have taken positive steps to provide much clearer information, for example on the placement of cookies. We want individuals to feel empowered to take control of their data and to report organisations to the Information Commissioner's Office (ICO) when they fail to comply with their obligations under the GDPR.

We will continue to support the ICO's efforts to work with organisations to improve compliance and take enforcement action where the circumstances of the case warrant it. The Government notes that the Competition and Markets Authority is also considering some of these issues in their ongoing market study into online platforms and digital advertising, and we look forward to their final recommendations.[1]

3. ***It is unreasonable to place the onus for knowing about the risks or harms associated with using web-based services on the consumer. Internet users should be able to trust that the infrastructure is secure and will protect them appropriately. Consent should no longer be used as a blanket basis for processing.*** **(Paragraph 27)**

Individuals, organisations and the government all have a responsibility for safety online. Cyber Aware is the UK government's campaign to help individuals and smaller organisations protect themselves online.[2] By promoting behaviours which help protect devices and online services, the campaign helps the public prevent unauthorised access to the vast amounts of personal information they store on their devices and online. This is crucial in light of how smartphones, computers and the internet have become such a fundamental part of modern life, from online banking and shopping, to email and social media. It is more important than ever for individuals to understand the steps they should take to prevent cyber criminals getting hold of their accounts, data, and devices.

However, while individuals should be aware of how to increase their safety online, the government agrees that it is not reasonable to put the onus solely on them. Organisations should be working hard to ensure that they design and maintain services which are secure and protect users from harm. Article 32 of the GDPR imposes specific obligations in this regard which are discussed in more detail in response to the Committee's recommendation 19. The National Cyber Security Centre provides a wide range of advice on cyber security to help organisations develop secure services and protect the data they hold.

1 Competition and Markets Authority, 'Online platforms and digital advertising market study' https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

2 Cyber Aware https://www.ncsc.gov.uk/section/information-for/individuals-families

4. ***Just as they do in the offline world, the Government must ensure robust regulatory standards are in place, and rigorously enforced, so internet users can be confident that any data that companies hold about them is being used in a reasonable manner.*** **(Paragraph 28)**

31. ***The GDPR should offer a substantial level of protection for people's personal data, but this does not seem to have materialised in practice. The Government should review whether there are adequate measures in place to enforce the GDPR and DPA in relation to how internet companies are using personal data, including consideration of whether the ICO has the resources necessary to act as an effective regulator*** **(Paragraph 105)**

The GDPR and the DPA 2018 set higher standards for organisations processing individuals' data, together with a much tougher enforcement regime. The new regime gives the ICO the power to fine companies up to £17 million[3] or 4% of total worldwide annual turnover, whichever is greater. This is compared with the previous maximum fine of £500,000 under the Data Protection Act 1998. As well as monetary penalties, the ICO has the power to issue information, assessment and enforcement notices (including ordering organisations to stop their processing of personal data), conduct audits, issue guidance and bring criminal prosecutions. Their approach to regulating data protection is set out in their Regulatory Action Policy.[4]

The DPA 2018 modernised the ICO's range of enforcement powers, partly in response to the increasing complexity of data processing activities in the 21st century and challenging cases like Facebook/ Cambridge Analytica. For example, if an organisation refuses to comply with the ICO's request for information about an alleged data breach, the ICO can now seek a court order to enforce compliance. Failure to do so would amount to contempt of court. The ICO can also now impose urgent assessment notices, requiring an organisation to allow the ICO to enter its premises to inspect its processing activities straight away, and enforcement notices requiring an organisation to address risky processing activities with as little as 24 hours' notice.

The DPA 2018 also modernised some existing criminal offences and created some new ones to deal with the worst data breaches. For example, it is now an offence for a person to destroy, dispose of, conceal, block or falsify documents to frustrate an information or assessment notice imposed by the ICO. All offences in the DPA 2018 are now classified as 'recordable' in England and Wales, which means that the offence will be recorded on the police national computer.

If individuals have concerns about how an organisation is processing their personal data, they can raise their concerns with the ICO. In the period between the new legislation being introduced on 25 May 2018 and 1 May 2019, the ICO received over 41,000 data protection concerns from the public. This represented a significant rise in comparison to 2017/18. In their report 'GDPR: One Year On'[5] , the ICO state that these figures have been impacted by a greater awareness of individuals rights.

3 Under the GDPR, the maximum fine is up to €20 million, which works out as £17 million in today's exchange rate

4 Information Commissioner's Office, 'Regulatory Action Policy' https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

5 Information Commissioner's Office, 'GDPR: One year on', 30 May 2019 https://ico.org.uk/media/about-the-ico/documents/2614992/gdpr-one-year-on-20190530.pdf

As mentioned above, the legislation is still less than two years old and we cannot yet draw firm conclusions about its impact. Some of the ICO's most complex investigations (for example, the Facebook/ Cambridge Analytica case) are long running. It often takes time for the most complex cases to be concluded and for any appeals to work their way through the courts. However, the ICO has shown a willingness to impose increasingly large fines. As the number and frequency of such cases increase, this may send a strong signal to companies about the consequences of non-compliance. The Government will continue to work closely with the Information Commissioner to ensure she has the resources and enforcement powers she needs to be an effective regulator.

5. **Children and vulnerable adults are likely to find it particularly difficult to give meaningful consent, given the complexity of documents they are being asked to read. In addition, peer pressure to join the same social networks as their friends may make the 'take it or leave it' approach to consent especially problematic for children. (Paragraph 34)**

6. **We do not believe that it is reasonable to expect 13 year-olds to give informed consent to their personal data being processed. (Paragraph 35)**

7. **We also believe there is a very strong likelihood of those under 13 regularly 'consenting' to their data being used, given that there is no meaningful way for a company to determine the age of the person consenting. (Paragraph 36)**

The Government agrees with the Committee that special care is needed when online services are processing data of children. That is why, during passage of the Data Protection Bill, the Government supported proposals from Baroness Kidron to require the ICO to publish statutory guidance for online services likely to be accessed by children on standards of age appropriate design. This was included in what is now section 123 of the DPA 2018. The Information Commissioner submitted the 'Age appropriate design code' to the Secretary of State in November 2019 and the Secretary of State will lay it in Parliament as soon as reasonably practicable. The current version of the code has been published on the ICO website. The Government has notified the draft code under the Technical Standards and Regulations Directive ahead of parliamentary approval.[6]

The code provides practical guidance for online services which are likely to be accessed by children on how to design data protection standards into their services to ensure they are appropriate for use by, and meet the development needs of children of all ages. The code is relevant to websites, apps, programs, websites, games, community environments, and connected toys or devices with or without a screen that process personal data. It reflects the UK's obligations under the United Nations Convention on the Rights of the Child, which recognises that children need special safeguards and care in all aspects of their life. It also sets out practical measures and safeguards to ensure processing under the GDPR can be considered fair, lawful and transparent in the context of online risks to children.

The code sets out 15 standards of age appropriate design. The focus is on providing default settings which ensure that children have the best possible access to online services whilst minimising data collection and use, by default. It also aims to ensure that children who choose to change their default settings get the right information, guidance and advice before

6 Information Commissioner's Office, 'Age appropriate design code' https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

they do so, and proper protection in how their data is used afterwards. The code requires privacy information and other published terms, policies and community standards, to be concise, prominent, and in clear language suited to the age of the child. It also sets out that, depending on the age of the child and the risks inherent in the processing, services should prompt them to speak to an adult before they activate any new use of their data, and not to proceed if they are uncertain.

Once the code comes into force, section 127 of the DPA 2018 requires the Commissioner to take it into account when considering whether an online service has complied with its data protection obligations. The code may also be used as evidence in court proceedings and the courts will be required to take its provisions into account wherever relevant.

The code complements our wider work to protect children ahead of and alongside the new online harms regulatory framework. Our Online Harms White Paper sets out a programme of action to tackle content or activity that harms individual users, including children, primarily through the establishment of a duty of care on companies to improve online safety. The duty of care will be overseen by an independent regulator who will have strong enforcement powers to deal with non-compliance. The Government is committed to bringing forward the most comprehensive and coherent approach possible to protecting children online, and the code plays a key role in delivering this objective.

8. ***The general rule under Article 8 of the GDPR is an age of digital consent of 16. Protections for children in the UN Convention on the Rights of the Child should apply to all children under the age of 18. While the 'consent model' for data processing in the GDPR remains, the Government should urgently act to protect children by raising the age of digital consent to 16, and putting in place adequate protection for all those under 18 who access services online. In any case, consent should not be used as a basis for processing the data of children under the age of 16.*** **(Paragraph 37)**

The GDPR gives Member States the discretion to set the age of digital consent between 13 and 16. While developing the DPA 2018, we considered that the large educational, social and cultural benefits of allowing 13 - 16 year-olds access to web services without parental consent merited setting the age at 13. The UK was not alone in this position. Countries such as Denmark and Sweden also set the age at 13. Our focus is on working with regulators and internet service providers to ensure that young people, including those aged 13–16, can enjoy the benefits of the internet in a safe environment.

Even though the age of digital consent is set to 13 years old in the UK, there are still practical things parents can do to help keep children safe online and minimise the amount of personal data that they share.[7] For example, using parental controls can help block upsetting or inappropriate content and control purchases within apps. They can also help parents plan what time of day their child can go online and how long for and manage the content different family members can see.

Legitimate interests

9. **Article 6 of the GDPR states that there may be legitimate interest for the controller to process the data without consent where there is a relevant and appropriate relationship**

7 National Cyber Security Centre 'Information for individuals and families' https://www.ncsc.gov.uk/section/information-for/individuals-families

between the individual and controller. However, there is not sufficient clarity on how an organisation determines what is in its legitimate interest and how it overrides the individual's rights. (Paragraph 42)

10. ***Given that there is a lack of understanding among companies around the use and relevance of the legitimate interests basis, we consider that there should be clearer guidance to companies either issued from the ICO or the Government around when and how the legitimate interests basis can be used. We also consider that there should be a rigorous process to test whether companies are using legitimate interests appropriately.*** **(Paragraph 43)**

If organisations are relying on legitimate interests as a legal basis for processing personal data they must consider, on a case by case basis, whether the rights of individuals to privacy outweigh their own interests, and ensure the processing is necessary and proportionate. The ICO has published comprehensive guidance on the use of legitimate interests as a processing condition.[8] Organisations also need to comply with data protection principles on fairness and transparency. If an organisation obtained personal data from a third party, individuals should normally be informed about the nature and purposes of the processing within a month, so that they can exercise their rights over the data, where appropriate. This is covered in article 14 of the GDPR.

In addition, where organisations are using new technologies to process personal data (in reliance on legitimate interests or any other processing condition), they must complete a Data Protection Impact Assessment (DPIA) if the processing is likely to result in a high risk to individuals. Where an impact assessment confirms such a risk, the organisation must consult the ICO before the processing begins. The ICO has published extensive guidance on completing DPIAs and may take enforcement action against organisations which fail to comply with these requirements.[9]

The ICO are working with organisations and specific sectors to help them better understand their obligations. We will continue to work closely with the ICO to keep this area under review.

Risk to privacy

11. *This conclusion is addressed above in response to points 1–2.*

Sharing data without the subject's knowledge

12. **The evidence we heard suggests that people's data is routinely being shared and used without their consent, which clearly infringes on their right to privacy. (Paragraph 53)**

Any organisations that rely on consent for their data processing activities must ensure that people are given clear information about the purposes of the processing and who the data is being shared with, so that consent given is genuine and meaningful. Consent is not

8 Information Commissioner's Office, 'Legitimate interests' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

9 Information Commissioner's Office, 'Data Protection Impact Assessments' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

the only lawful basis for processing personal data. We discussed legitimate interests as a processing condition above and, depending on the circumstances, there might be other relevant legal bases available to the data controller under article 6 of the GDPR. But if personal data is being processed without any lawful basis then it would be in breach of the GDPR and the controller could be reported to the ICO and would be liable to enforcement action.

13. ***It should be made much simpler for individuals to see what data has been shared about them, and with whom, and to prevent some or all of their data being shared.*** **(Paragraph 54)**

14. ***The Government should explore the practicality and usefulness of creating a single online registry that would allow people to see, in real time, all the companies that hold personal data on them, and what data they hold.*** **(Paragraph 55)**

The current legislation strengthens people's rights to access, correct and erase personal data about them and to object to its processing. As set out above, organisations have a responsibility to ensure that they are presenting users with clear information about how, why and where their information is being processed, and how individuals can contact them if they would like to amend or erase their personal data. Through their 'Your data matters' campaign, the ICO provides individuals with information on how to exercise their rights.[10]

The Government is grateful for the Committee's recommendation, but respectfully disagrees that creating a registry including details of all the companies with whom data about individuals had been shared would be a positive step forward. Building, maintaining and administering such a registry would pose significant technical and financial challenges and, even if it were possible, it would involve the administrator processing even more personal data about individuals. Individuals who were concerned about the range of organisations who held their data and the nature of their processing activities would still need to contact those companies directly to seek access, rectification or erasure. In the Government's view, the focus should be on ensuring that online services are complying with the fairness and transparency obligations in the GDPR (including by informing individuals with whom data had been shared), so that people can make informed choices whether or not to continue using particular services.

Combining data from different sources

15. **Even where individuals have knowingly consented to sharing some of their personal data with one company, they may not be content with that data being combined to create a profile of themselves that they have no opportunity to see or edit. (Paragraph 64)**

16. **It is deeply concerning that 'data' about an individual is being used and shared when it is based on inferences that may be untrue, and when the individual has no opportunity to correct any inaccuracies: indeed, there is no way of finding out what inferences may have been made about you. (Paragraph 65)**

10 ICO guidance 'Your data matters' https://ico.org.uk/your-data-matters/

17. **This makes the need for people to be informed about what data is being collected and shared, and with whom, even more pressing. (Paragraph 66)**

18. ***We agree with the recommendation of the House of Lords Communications Committee that, in a model similar to a subject access report under the GDPR, users should have the right to request data that a company has generated about them, so they are aware of any inferences that may have been made.*** **(Paragraph 67)**

25. ***Important decisions—such as whether to refuse someone access to a service—should never be made based on inferences from people's data, and the Government should review whether the current legal framework is adequately robust in this regard.*** **(Paragraph 89)**

The GDPR requires data controllers to be clear with individuals, at the point of data collection, how and why their personal data is going to be used. Controllers also have a duty to tell individuals about data they have received from third parties within a month of receiving it. The right of access under article 15 of the GDPR includes the right to information about the existence of any automated decision-making, including profiling, that will use their personal data. This includes meaningful information about the decision-making process, as well as the significance and expected consequences of such processing for the individual. Organisations which fail to comply with these obligations can be reported to the ICO who may wish to consider enforcement action.

As the Committee highlights, many organisations are using data, not all of which has been provided directly to them by data subjects. Organisations might make assumptions about individuals based on data they have obtained from third parties or conclusions they have drawn from a person's viewing habits, location or preferences. Commonly referred to as "inferred data", organisations can undertake analytics which enables them to draw inferences which may then be used to categorise users and, for example, serve them more tailored content, calculate credit scores or predict future health outcomes. However, information which has been inferred about an individual is still personal data for the purposes of the GDPR and there are requirements in article 5(1)(d) of the GDPR to ensure that any personal data held is accurate.

The Government agrees with the Committee that there are significant risks for individuals if automated decision-making and profiling are used irresponsibly. That is why article 22 of the GDPR, as supplemented by section 14 of the DPA 2018, gives people the right to object to such decisions and request human intervention. Section 14 applies if an organisation makes a decision based solely on automated processing which has legal or other similarly significant effects for a data subject, unless the processing was necessary to fulfill a contract between the organisation and the data subject, or the data subject gave explicit consent. If section 14 applies, the organisation must contact the data subject within a month of making the decision, so that the individual can decide whether to require the organisation to reconsider the decision or take a new decision that is not based solely on automated processing. Where data controllers are not complying with their responsibilities under the legislation they should be reported to the ICO.

We agree with the Committee that this is an important issue and, while the use of big data sets brings valuable benefits, data subjects should feel confident that they understand how decisions about them are being made. The ICO has produced guidance on this subject -

'Big data, artificial intelligence, machine learning and data protection'.[11] This explains the various categories of data which are involved in these activities and the responsibilities on organisations to meet their data protection obligations. They have also produced guidance on automated decision-making and profiling to help organisations apply data protection requirements to these activities.[12]

Risk of data breaches

19. ***Companies hold significant amounts of our personal data. They must take full responsibility for keeping it safe and secure.*** **(Paragraph 70)**

As mentioned in response to recommendation 3, the GDPR has strengthened the legal requirements concerning the security of personal data. Article 5(1)(f) of the GDPR requires controllers to ensure that personal data is "*processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*".

There are also specific requirements under article 32 of the GDPR for organisations to consider their physical and organisational security measures, as well as their cyber security. It is for each organisation to ensure that they have suitable security measures in place, proportionate to the risk, as they will all operate in different contexts. In the event an organisation's security is breached, they must report it to the ICO within 72 hours under article 33 of the GDPR, unless the breach is unlikely to result in a risk to the rights of individuals.

The ICO has produced guidance to support organisations with their information security. The National Cyber Security Centre has also published advice and guidance to support organisations with their cyber security, for example, their '10 steps to cyber security' guidance[13] and launched the Cyber Essentials scheme[14] which enables organisations to demonstrate whether they have met basic cyber security controls.

If an organisation fails to comply with any of its obligations under Articles 25 to 36 GDPR, they are in breach of the legislation and liable to enforcement action.

User choice?

20. **Companies must respect people's right to privacy, and make it easier for people to limit or stop how their data is being shared. (Paragraph 74)**

We strongly agree with protecting people's right to privacy and their other data rights, as set out in existing legislation. If a company is sharing personal data with third parties based on the data subject's consent, the data subject can withdraw that consent at any time.

11 ICO guidance 'Big data, artificial intelligence, machine learning and data protection' https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

12 ICO guidance 'Automated decision-making and profiling' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/

13 The National Cyber Security Centre, '10 steps to cyber security' https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security

14 The National Cyber Security Centre, Cyber Essentials https://www.cyberessentials.ncsc.gov.uk/

If a company is sharing personal data based on legitimate interests overriding the data subject's privacy rights, article 21 of the GDPR gives the data subject the right to object to the sharing of their personal data at any time. This effectively allows individuals to stop or prevent an organisation from sharing all or a subset of their personal data, unless there are compelling legitimate grounds for the sharing to continue. An individual's objection may relate to a particular purpose the organisation is processing the data for.

Finally, if an organisation fails to comply with reasonable requests, the individual may refer their complaint to the ICO who may investigate further.

Challenging or deleting data

21. ***Given that many people will have consented to their personal data being shared without being in a position to understand what they were agreeing to, that people's data is being shared without their consent and that inferences are being drawn from people's data to create a profile of them that may be entirely incorrect, it is vital that companies make it easy for people to correct or remove data held about them. While the GDPR gives individuals the rights to have their personal data erased and rectified, the evidence we heard suggests that these are not always adequately enforced. Companies must respect people's right to privacy, and make it easier for people to limit or stop how their data is being shared. We consider that these rights could be more effectively enforced if specific sanctions were associated with non-compliance of these rights by companies, particularly when companies fail to respond promptly or adequately to individual's requests to rectify or delete their data.*** **(Paragraph 78)**

Article 5(1)(d) of the GDPR requires organisations to ensure that personal data is accurate and up-to-date, and to take every reasonable step to ensure that personal data that is inaccurate is erased or rectified without delay. Individuals have specific rights under article 16 of the GDPR to seek the rectification of their data. The Committee suggests that these rights could be more effectively enforced if there were specific sanctions for non-compliance, but a failure to comply with article 5 of the GDPR or a refusal to respond to reasonable request for rectification could already lead to enforcement action by the ICO. In addition, the ICO must progress complaints in a timely manner.

The risk of discrimination

22. ***We were shocked to hear that major companies have used the ability to target advertising in order to discriminate against certain groups of people. Those social media channels and websites on which the advertisements are being placed must accept responsibility and carry out sufficient checks on adverts to ensure that companies are not inadvertently or deliberately excluding people in a discriminatory way which disadvantages them in their access to opportunities in areas like employment, housing or finance.*** **(Paragraph 86)**

23. ***There are challenging questions to be asked about the balance between providing 'personalised content' (i.e. showing someone the advertisements, news stories etc. that they are most likely to be interested in) and discriminating against people by deciding certain material should or should not be shown to them because of their particular demographics. This debate needs to be had, and we urge the Government to bring***

internet companies, regulators and users together to discuss this. These discussions should also explore how anti-discrimination laws can be better enforced in the online advertising world. **(Paragraph 87)**

24. ***Companies need to be aware of how targeting content at people based on certain hobbies, interests etc may indirectly be discriminating against certain groups of people. They should be actively looking for, and screening out, such practices and ensuring they have adequate tests in place to consider whether targeting certain aspects of users' profiles could be discriminatory.*** **(Paragraph 88)**

The Equality Act 2010 prohibits service providers from discriminating against people on the grounds of protected characteristics.[15] A court may grant civil remedies to individuals who have been victims of such discrimination.

The Government and other bodies are actively considering issues around online targeting. This includes: the ICO's report on "adtech" and real time bidding;[16] ongoing reviews by the Centre for Data Ethics and Innovation into online targeting[17] and bias in algorithmic decision making;[18] and the market study currently being undertaken by the Competition and Markets Authority into online platforms and the digital advertising market in the UK.[19] In addition the Government recently published a call for evidence to help consider how online advertising is regulated.[20]

25. *This recommendation is addressed above in response to points 15–18.*

26. ***We consider that more transparency is needed in relation to how advertisements are targeted at individuals online, in order to prevent discrimination from occurring. This could potentially include introducing tools through which individuals can look up how companies are targeting adverts at them, or at others, online and which would enable regulators to effectively audit the criteria used by advertisers.*** **(Paragraph 90)**

We agree with the Committee that this is an important issue. The Government supports transparent and ethical targeting practices for advertising online, so that consumers are informed, empowered and can have trust in online advertising. We recognise the growing number of industry-led initiatives and software that exists to promote transparency, but acknowledge the need for further progress, and are considering this issue. As referred to above, other bodies are also considering the matter. For example, the ICO has undertaken work looking specifically at adtech and real time bidding. Through this work, they have found transparency to be a significant issue and are now considering whether regulatory intervention is required.

15 Protected characteristics are age, gender reassignment, marital status, being married or in a civil partnership, being pregnant or on maternity leave, disability, race including colour, nationality, ethnic or national origin, religion or belief, sex, or sexual orientation

16 Information Commissioner's Office, 'Update report into adtech and real time bidding', June 2019 https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

17 Centre for Data Ethics and Innovation, 'CDEI Review of Online Targeting', February 2020 https://www.gov.uk/government/publications/cdei-review-of-online-targeting

18 Centre for Data Ethics and Innovation, 'Interim report: Review into bias in algorithmic decision-making', July 2019 https://www.gov.uk/government/publications/interim-reports-from-the-centre-for-data-ethics-and-innovation/interim-report-review-into-bias-in-algorithmic-decision-making

19 Competition and Markets Authority, 'Online platforms and digital markets market study' https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

20 Department for Digital, Culture, Media and Sport, 'Online advertising - call for evidence', January 2020 https://www.gov.uk/government/publications/online-advertising-call-for-evidence/online-advertising-call-for-evidence

27. **We consider that mechanisms allowing for better collective redress could be particularly useful in relation to targeted advertisements online, given that an individual cannot compare what they see online with what is seen by others and would therefore be unaware that they were being discriminated against. In such situations, unlawful practices are more likely to be revealed by independent investigations, most often carried out by civil society organisations and charities; if these organisations could then pursue cases on behalf of the affected individuals, the companies undertaking these activities could more effectively be held to account. (Paragraph 92)**

Article 80 of the GDPR and section 187 of the DPA 2018 give individuals the right to ask certain not for profit organisations to act on their behalf to complain to the ICO. The provisions also permit such organisations to seek a tribunal order to require the ICO to progress a complaint; or a court order to require data controllers to comply with the law or pay compensation for loss or damage. Section 189 of the DPA 2018 requires the Secretary of State to review the effectiveness of these provisions and consider whether they should be extended to actions brought on behalf of individuals who have not given their specific authorisation. The Government intends to launch a call for views in the spring with a view to laying a report before Parliament by November 2020.

The UN Guiding Principles

28. **The UN Guiding Principles on Business and Human Rights, if fully implemented, would address many of the concerns raised in this report by requiring companies to both make users aware of how their data is used and proactively identify and mitigate any adverse impact their activities may have on people's human rights. (Paragraph 98)**

The Government supports the UN Guiding Principles on Business and Human Rights, which are the authoritative international framework on these issues. We were the first country in the world to bring forward a national plan for the Guiding Principles. The Guiding Principles are a voluntary framework which recognises that States have discretion to decide what mix of measures—national and international, mandatory and voluntary—should be used to prevent, investigate, punish, and redress human rights abuses by private actors. Our National Action Plan follows this approach and combines targeted regulation, like the Modern Slavery Act 2015, to influence behaviour, with other initiatives like support for the business-led Human Rights Benchmark, to help drive this important agenda. Respect for human rights should be at the heart of doing business responsibly, but the Government recognises that this poses varying challenges to different businesses, so the National Action Plan mirrors the Guiding Principles by confirming broad expectations applicable to all business: namely, that they should integrate respect for human rights across their operations including their data management.

29. ***The Government should consider how it could mandate internet companies to adhere to the Guiding Principles, and how it could effectively enforce such a requirement. We restate the recommendation from our 2017 report on business and human rights that reporting on due diligence in human rights should be compulsory for large businesses.*** **(Paragraph 99)**

The Government wants our large UK businesses to be transparent about their policies, activities and impacts, and to report on human rights issues and risks, as appropriate, so that consumers, investors and campaigners alike can hold them to account. The

Companies Act was amended in 2013 to require our listed companies to cover material human rights impacts in their annual reports, where relevant for understanding of the business; and this was strengthened in 2016 to provide a fuller framework for strategic reporting, including to cover due diligence arrangements, where these are in place. In parallel, our large companies are now expected under the Modern Slavery Act 2015 to publish annual statements on how they guard against this appalling human rights abuse across their supply chains.

30. ***The Government should also update its National Action Plan for implementing the Guiding Principles to include specific consideration of the impact of internet and social media companies on human rights.*** **(Paragraph 100)**

The Government is committed to deliver on the approach of its National Action Plan and to stay in touch with stakeholders as we continue this. The Government is clear that wide consultation must inform any future development of the approach, so we welcome discussions with businesses and civil society organisations on this.

Stronger enforcement of regulation

31. *This recommendation is addressed above in response to recommendation 4.*

New regulation

32. ***While we welcome the publication of the Government's Online Harms White Paper, it was disappointing that violation of people's right to privacy and freedom from discrimination were not included in their list of online harmful activity that they consider to be in scope of the White Paper. We do not agree with the Government that the existing legal framework provides adequate protection against the misuse of people's data by internet companies and would urge them to reconsider the scope of their proposals.*** **(Paragraph 108)**

33. ***The Government's proposals to create a new statutory duty of care to make companies take more responsibility for the safety of their users, enforced by an independent regulator, could provide a valuable framework for ensuring that internet companies uphold people's human rights. We urge the Government to include in its proposed "duty of care" a requirement for companies to adhere to robust standards on how people's data is processed.*** **(Paragraph 109)**

34. ***The Government should also consider how the UN 's Guiding Principles on Business and Human Rights could be incorporated into their new regulatory regime.*** **(Paragraph 110)**

The UK is committed to a thriving economy, driven by world-leading digital technology and a society in which technology works to the benefit of all citizens, and where the UK is the safest place in the world to be online. To support this ambition, the government is leading work to develop an ambitious strategic approach to regulating and governing digital technologies.

The Government believes that the UK's data protection legislative framework provides robust protection of people's privacy and personal data, and imposes high standards for

how people's data is processed which companies, including those that operate online, must meet. The regulatory framework outlined in the Online Harms White Paper is focused on how online companies handle user-generated content and activity rather than on how companies use people's data. The White Paper makes clear that the new regulatory framework will not cover harms resulting from breaches of the data protection legislation.

We expect that the new regulator's work will allow people to better exercise their right to freedom from discrimination owing to the new regulator's work. Vulnerable groups, including children, older people, religious and ethnic minorities, LGBT+ people and people with disabilities are disproportionately affected by online harms. The Government's proposed new online harms regulatory framework will ensure that vulnerable groups can benefit from the opportunities offered by the internet and seek redress when subject to harm. As a public body, the new regulator will be subject to the public sector equality duty in Section 149 of the Equality Act 2010. This requires public bodies and others carrying out public functions to have due regard to the need to eliminate discrimination, to advance equality of opportunities and foster good relations.

The duty of care is intended to ensure companies take more responsibility for tackling harm caused by user-generated content and activities on their platforms. It will be for the independent regulator to set out the steps companies can take to fulfil the duty of care in codes of practice.