DATA THE WRONG DIRECTION

All the issues we expect to see in the UK Data Reform Bill

In this document

0. EXECUTIVE SUMMARY

On June 17, the UK Government published their response to Data: a new direction, outlining their plans to scrap the UK GDPR and replace it with a "UK Data Reform Bill".

Open Rights Group took part in the consultation process, emphasising how the proposals in Data a new direction would have significantly undermined legal standards, disempowered individuals, and removed effective remedies and oversight against abuses. We also denounced the Department of Digital, Culture, Media and Sport together with more than 30 civil society organisations, lamenting their cherry-picking and arbitrary engagement with stakeholders of their choice.[1]

Among wrong premises and a rigged process, the consultation response unsurprisingly validates much of the fears and criticism that other organisations and we have voiced. In particular, this analysis focuses on how the UK Data reform Bill would:

- Erode the principles of lawfulness and purpose limitation, by expanding Government powers to amend the rules arbitrarily;
- Disempower individuals, and reduce or significantly hinder the exercise of fundamental rights such as the right of access, the right to a human review, the right to privacy in electronic communications and the right to lodge a complaint;
- Lower the level of protections in the context of International Data Transfers, with the implicit aim of tying transfers mechanisms to trade agreements;
- Reduce accountability to a hollow box-ticking exercise, where organisations are free to choose how to demonstrate compliance with the law and self-evaluate their efforts;
- Undermine the independence of the Information Commissioner's Office, while tasking their office with burdensome and conflicting duties that will hinder their ability to enforce the law effectively.

Finally, take stock of the changes proposed in the UK Data Reform Bill, revealing how these provisions would work in unison to create a brave new digital police state, undermine innovation to favour the cronies and the law-breakers, and create a hostile environment for victims of data-driven harms and discrimination.

1 Techmonitor AI, *Data Reform Bill consultation 'rigged' say civil rights groups*. Available at: https://techmonitor.ai/policy/privacy-and-data-protection/data-reform-bill-consultation-dcms-nadine-dorries

1. LAWFULNESS AND PURPOSE LIMITATION

Article 8 of the European Convention of Human Rights provides that interferences with one's private life must be authorised by law, have a legitimate scope, and be surrounded by safeguards against abuses. In the UK GDPR, this is reflected by the principles of lawfulness: Personal data shall be processed under the conditions set by six lawful grounds for processing (Article 6).

Furthermore, honouring individuals' reasonable expectations over data processing helps preserving trust, legal certainty, and the rule of law. In the UK GDPR, this is reflected by the principle of purpose limitation: personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Instead, Data: a new direction builds on the assumption that data must be "unleashed" to generate value across the economy; thus, it wants to normalise and make it easy to reuse personal data beyond the original purpose of collection.

In the following sections we explain how the UK Data Reform Bill would:

- Empower the Government to arbitrarily introduce new grounds for processing, thus undermining the principle of lawfulness (1.1 Undermining lawfulness);
- Empower the Government to introduce arbitrary derogations from the principle of purpose limitation, and for organisations to reuse and share personal data in ways individuals would not expect (1.2 Undermining purpose limitation);
- Shape a regulatory environment that favours reckless behaviour, arbitrariness and cronyism (1.3 Impact of proposed changes)

1.1 Undermining lawfulness

In the UK GDPR, six lawful grounds for processing provide clear and objective conditions that define legitimate uses of personal data. For instance, data processing will be legitimate:

To fulfil a legal obligation, a contractual obligation, carry out a task in the public interest, or to save the life of the individual, insofar data processing does not exceed what is reasonably needed to fulfil these tasks;
If individuals have agreed to their data being used, insofar they were free to choose and were given the information to understand the consequences of their choices;

In the interest of the organisation using this data, insofar they carried a balancing test to demonstrate that this activity does not trump the rights and freedom of the individuals concerned. In other words, they will have to demonstrate that these activities are uncontroversial, or that they are using precautions to protect individuals from harm and abuse.

Instead, the UK Data Reform Bill intends to empower the UK Government with "regulatory-making power to introduce and update a list of legitimate interests activities for which organisations could use personal data without applying the balancing test", initially "limited to

- processing activities which are undertaken by data controllers to prevent crime or report safeguarding concerns, or
- which are necessary for other important reasons of public interest" (Q1.4.1, 1.4.2, 1.4.3, 1.4.4).

In essence, this "regulatory-making power" would allow introducing new lawful grounds for processing, and:

- Firstly, **it would reduce legal certainty:** boundaries and conditions that define what is legitimate and what is unlawful would be defined by the Government at will, to the extent and at the time of their choosing.
- Secondly, **it would reduce public scrutiny:** these "legitimate interests" would be introduced with secondary legislation, thus with little Parliamentary scrutiny and debate.
- Thirdly, **this new "regulatory-making power" would be open-ended and unfettered:** the Government propose "to create a power to update the list of activities in case other processing activities are identified that should be added to the list";
- Fourthly, **legitimate interest in its current form empowers organisations** and the Government to think about the processing they intend to do, the impact on people at the outset, and the measures that can be taken to mitigate risks (safeguards, data minimisation, security, accountability).

1.2 Undermining purpose limitation

In the UK GDPR, organisations have to be clear and open about the reasons for obtaining personal data, and that their use is in line with the reasonable expectations of the individuals concerned.

Article 23 of the UK GDPR already allows to introduce legislative measures that allow the reuse of data for incompatible purposes for reasons of general interests.

However, this law must “meet an objective of public interest and be proportionate to the legitimate aim pursued”, and specify

- The extent (purposes, category of personal data, organisations) and scope to which such exemption would apply;
- The safeguards to prevent abuse or unlawful access or transfer;
- The storage periods and the applicable safeguards.

In other words, Article 23 mandates strict safeguards against abuses and ensure these restrictions are not irreversible.

Instead, in the UK Data Reform Bill intend to

- Allow the reuse of data, in breach of the purpose limitation principle, when “based on a law that safeguards an important public interest” (question 1.3.2)
- Clarify the compatibility test (question 1.3.2)

In essence, **this would empower the Government to restrict the principle of purpose limitation via secondary legislation, without the need to implement the safeguards provided in Article 23 of the UK GDPR.**

Also, while little explanation is given about how the compatibility test would be clarified, the Government claim that “uncertainty among organisations’ compliance and legal teams regarding the rules on the re-use of personal data had led to delays in advancing research efforts or innovations”. This suggest the intention to ease the compatibility test to allow a more liberal use of personal data across the board

2. DATA PROTECTION RIGHTS

In the UK GDPR, individuals have rights that allow them to exercise greater control over the use of their personal information. This mitigates power imbalances between individuals and organisations. These rights include

- The right of access;
- The right not to be subject to decisions based solely on automated processing that may result in legal or otherwise significant effects;
- The right not to be tracked (on the internet) unless individuals consented to cookies being stored on their devices.
- The right to lodge a complaint with the ICO.

Instead, Data a new direction builds on the assumption that SARs are time consuming and costly for organisations, that Article 22 may be a barrier to the development of AI, that cookie banners are unnecessary, and that the ICO spend too much time on handling data subjects' complaints.

In the following sections we explain how the UK Data Reform Bill would:

- Restrict the right of access, and allow organisations to question the motives of, reject a subject access request, or charge a fee (2.1 Restricting the right of access);
- Remove the general prohibition against solely automated decisions in Article 22, and reframe it as a right to have certain safeguards over automated decisions (2.2 Watering down the right to human review);
- Make online spying the default option, and switch from an opt-in to an opt-out model for the storage of cookies that track and profile users (2.3 Removing the right to privacy in electronic communications);
- Impose burdensome requirements on individuals filing complaints, and empower the ICO to arbitrarily dismiss complaints where the complainant has not first attempted to resolve the issue with the offender (2.4 Hindering the right to lodge a complaint);
- Shape a regulatory environment to protect organisations from the concerns of individuals rather than protecting individuals from harmful uses of data (2.5 Impact of proposed changes).

2.1 Restricting the right of access

In the UK GDPR, individuals

- Have the right to access and receive a copy of their data. Subject access requests (SARs) enable control over personal data. It allows individuals to understand how their data is being processed, the consequences of such processing, and to verify the legitimacy of data uses.
- Do not need to justify the reason for their request, and organisations cannot charge individuals for exercising their rights unless they can prove that their request is "manifestly unfounded or excessive";

Instead, the UK Data Reform Bill intends to lower the current threshold for refusing or charging a reasonable fee for a subject access request from "manifestly unfounded or excessive" to "vexatious or excessive", to bring it in line with the Freedom of Information regime (Q2.3.2). The test in the FOIA regime permits to take into account the context and history of a request, including the identity of the requester and any previous contact with them. Furthermore, it allows organisations to request information concerning the purpose of a request and to narrow its scope.

In essence, this regime would reframe subject access requests as a protection in favour of organisations whose activities may be concerning for others. This would disempower individuals and undermine transparency as follows:

- Firstly, **FOIA and SAR regime serve very different purposes.** FOIA enable individuals to seek access to "information held by public authorities or by persons providing services". Importantly, individuals seek information tied to public services and projects that are already known. In contrast, the subject access regime is designed to allow people to be informed about how their data is being used, something that they may not otherwise know about. Thus, it is inherently speculative.
- Secondly, **the UK GDPR access request regime already allows organisations to refuse a request if it is malicious** or if the access request is being used to harass the organisation and cause disruption. On the other hand, the threshold is intentionally high, to ensure access requests are not unfairly rejected.
- Thirdly, **allowing organisations to request information on the purpose of a request will intimidate individuals who have less power or are in a position of vulnerability**. Also, an individual may just want to know and understand what personal data is being used and why, without any wider purpose behind their request.
- Finally, **the same threshold would allow organisations to charge a fee to act upon your request.** Contrary to the Government response that they do not "intend to re-introduce a nominal fee for processing subject access requests", the same issues we listed above would apply in this scenario.

2.2 Watering down the right to human review

In the UK GDPR, individuals have the right not to be subject to decisions based solely on automated processing that may result in legal or otherwise significant effects. Article 22 of the UK GDPR:

- Protects individuals against significant risks that profiling and automated decision-making can pose;
- Equates to a general prohibition, as it would be unfair to require the data subject to proactively seek an objection to a decision taken by an automated system they are not responsible for or in control of.

Instead, the UK Data Reform Bill intends to remove the right to human review for solely automated decisions, and replace it with "a right to specific safeguards, rather than as a general prohibition" (Q1.5.14, 1.5.15, 1.5.16, 1.5.17).

- **Watering down the right a human review of automated decision-making is concerning** given the trend towards the greater digitalisation of our society, with more and more decisions being made or helped by AI, as:
- **AI is increasingly being used for sorting citizens into social hierarchies**, for exclusionary or discriminatory purposes;
- **Article 22 has been a key safeguard against automated and unfair dismissals or wage deductions.** Also, automated decision-making is increasingly used to determine whether people should receive benefits, thus the importance of Article 22 is bound to increase over time;
- **Issues identified in the consultation response, such as confusion over the meaning of "solely" or "significant effect" can be addressed by relying on the EDPB guidance on Article 22.** This means strengthening rather than lowering the protections afforded by Article 22, in line with the opinions expressed by respondents in Data a new direction.

2.3 Removing the right not to be tracked

The Privacy in Electronic Communications Regulations (PECR) regulates the use of cookies. In essence, it provides the right not to be subject to online tracking and profiling, unless the individual agrees. This is an important safeguard against the ever-growing pervasiveness of Internet tracking and profiling, as it protects individuals from the harmful and discriminatory effects of these practices.

Instead, the UK Data Reform Bill would move to "an opt-out model of consent for cookies placed by websites" where "cookies could be set without seeking consent"

but only after "browser-based and similar solutions" are widely available (Q2.4.1, 2.4.2, 2.4.3, 2.4.4, 2.4.5, 2.4.6, 2.4.7, 2.4.8).

- **Cookies enable widespread and uncontrolled surveillance and behavioural profiling of individuals,** which have resulted in real-world harms. For instance, gambling operators are able to use cookies to profile and target vulnerable individuals with gambling addictions.
- **This reform would facilitate and legitimatise some of the most harmful practices online.** This is inconsistent with the government's position on online harms and would lead to a proliferation of online and real-world harms.

2.4 Hindering the right to lodge a complaint

In the UK GDPR, individuals have access to judicial and administrative remedies, including the right to lodge a complaint with the ICO. Formal complaints are an essential means to hold controllers responsible and enable data subjects to challenge violations of their rights.

Instead, the UK Data Reform Bill intends to give the ICO "clear discretion in legislation not to investigate certain types of data protection complaint, including vexatious complaints, and complaints where the complainant has not first attempted to resolve the issue with the relevant data controller". This discretion would be granted "alongside a requirement on data controllers to have a simple and transparent complaints-handling process in place to deal with data subject complaints." (Q5.6.1, 5.6.2, 5.6.3, 5.6.4).

These proposals would substantially lower individuals' access to administrative remedies for the misuse of their data, since:

- Individuals will need to lodge a complaint with the offender first. **Such complaint-handling procedures would be privatised and likely weaponised to misrepresent facts and discourage individuals from exercising their rights.** This process also presents the risk of complainants making procedural mistakes that the ICO can weaponise to ditch their complaint.
- **There are instances where the complexity and opaqueness of digital ecosystems make it difficult, if not impossible, to identify an organisation to complain against.** For instance, personal data may be processed and shared among a vast network of intermediaries which lack a direct relationship with the individuals concerned, or do not provide sufficient transparency to allow their identification.
- The current regime allows for a degree of predictability and foreseeability in what the Commissioner can and cannot do in response to a complaint.

Introducing a proportionality test would introduce uncertainty and possibly inconsistent decision making, thus leading to uncertainty for individuals;

- **The Commissioner rarely takes enforcement action against data controllers even when widespread or systemic issues are highlighted.** Instead, the Commissioner focuses on practices that may result in higher risks to individuals, such as in the data broker industry or the democratic process. This position can frustrate data subjects. **The protection afforded to individuals would be reduced if the Commissioner is granted further discretion.**

3. INTERNATIONAL DATA TRANSFERS

Safeguards around international data transfers are a fundamental component of data protection laws. Digital technologies and the Internet make it more likely that personal data may be stored or transferred outside of the UK GDPR jurisdiction: thus, ensuring that data protection rights "follow the data" is an essential safeguard against loopholes and data laundering.

Instead, Data a new direction builds on the premises that "Data flows have a larger impact in raising world GDP than the trade in goods", and thus aims "to facilitate digital trade [...] by agreeing to commitments in bilateral and plurilateral trade agreements".

In the following section, we explain how the UK Data Reform Bill would approach the discussion of adequacy almost entirely in terms of supporting the free flow of data, whilst failing to acknowledge the need to provide adequate protection for personal data.

3.1 Boosting data laundering

In the UK GDPR, transfers may take place if the third country ensures an adequate level of protection. Usually, this will require:

- An adequacy decision, where a Country legal system has been deemed to offer an essentially equivalent level of protection to the UK GDPR;
- Alternatively, the organisation that transfers data oversea will have to provide appropriate safeguards through technical or legal means, such as standard data protection clauses or binding corporate rules.

In essence, this framework ensures that individuals retain enforceable data rights and legal remedies regardless of the position their data is being stored.

The Data Reform Bill intends to make the UK International Transfer Framework "risk based" (Q3.2.1) and in particular to

- Relax "the requirement to review adequacy regulations every 4 years", and give discretion to the Government as to when and why to initiate a review (Q3.2.3);
- Consider administrative remedies as "adequate" safeguards for data transfers, even if there is no judicial remedy available (and vice versa) (Q3.2.4);
- Introduce "a new power for the DCMS Secretary of State to formally recognise new alternative transfer mechanisms"(Q3.3.7, 3.3.8), which will admittedly include using adequacy for groups of countries, regions and multilateral frameworks "in the future, especially as it seeks to prioritise work on multilateral solutions for data flows" (Q3.2.2)

Furthermore, the Government intend to introduce a risk-based approach to data exporters “when using alternative transfer mechanisms” (Q3.3.1, 3.3.2).

Introducing a risk-based approach to data transfers constitutes a significant weakening in data protection rights, and a departure from Schrems II. Indeed:

- **A risk-based approach to international data transfers has consistently been rejected by Data Protection Authorities in the EU.** The EDPB also reached the conclusion that an essentially equivalent level of protection of personal data requires such protections to be enforceable in practice.
- **The Government are planning to strike deals with countries which do not provide adequate protection to personal data**, such as the United States, Australia, and Singapore;
- **Schrems I ruled that the availability of independent and impartial judicial remedies is a key consideration for adequacy status**, but the UK Data reform Bill intends to remove this requirement.

4. ACCOUNTABILITY

Accountability promotes the enforcement and effective implementation of data protection rules. It is also a proactive requirement, as carrying out assessments helps organisations to identify harmful or discriminatory outcomes.

In the UK GDPR, the accountability framework requires organisations to implement appropriate and effective measures that translate principle and obligations enshrined in legislation into practice. Importantly, it includes risk-based but prescriptive requirements that organisations have a duty to demonstrate upon request. While voluntary accountability measures are encouraged, prescriptive requirements ensure that individuals and the ICO can test compliance with the rules and the effectiveness of these measures.

Instead, Data: a new direction builds on the assumption that accountability is a "key driver of unnecessary burdens on organisations".

In the following section, we explain how the UK Data Reform Bill would establish confusing and uncertain accountability requirements, in turn undermining the effective implementation and enforceability of data protection law.

4.1 Scrapping the accountability framework

In the UK GDPR, the controller is responsible for, and must implement technical and organisational measures to ensure, and be able to demonstrate, that processing is carried out in accordance with the law. Among these measures:

- The appointment of data protection officers (DPOs), who must not receive any instructions and must not be dismissed or penalised in any way for performing their tasks when advise on compliance with data protection rules;
- The keeping of records and documentation (ROPAs), which is intended to ensure that the ICO will have the necessary documentation to enable them to confirm the lawfulness of processing;
- The conduct of data protection impact assessments (DPIAs), that enables organisations to properly identify, address and mitigate the risks in advance, thus limiting the likelihood of a negative impact on individuals as a result of the processing;
- The requirement to consult the ICO if, after conducting a data protection impact assessment, risks could not be mitigated.

These requirements are risk-based, and are mandatory only when processing activities present a given level of risk (DPIAs, DPOs), or when the organisations or the scale of data processing reach a certain threshold (DPOs, ROPAs).

Instead, the UK Data Reform Bill intend to

- Scrap the accountability framework, and replace it with privacy management programmes that lack any meaningful definitions;
- Remove the requirement to appoint and independent DPO, and require "appointing a suitable senior individual" to be responsible for carrying out privacy management programmes;
- Remove the requirement to carry out DPIAs and ROPAs, and give freedom to organisations to decide when and to what extent to keep documents or assess risks;
- remove the mandatory requirement for organisations to consult the ICO prior to any high-risk processing activity, and instead make voluntary prior consultation with the regulator a mitigating factor which the ICO may take into account when taking any enforcement action against an organisation.

(Q2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.2.5, 2.2.6, 2.2.7, 2.2.8, 2.2.11, 2.2.16)

This would undermine the effective functioning of accountability in the following manners:

- **Existing accountability requirements under the UK GDPR played a significant role in holding offenders to account and obtaining remedies against the violation of data protection rights.** Prescriptiveness allows individuals and regulators to know what to look for, and provides comparable standards to evaluate the reliability of these measures.
- **Where the risk threshold is met, the UK GDPR sets out clear obligations which promote legal certainty, including when it comes to enforcement.** The Government misconstrue this as a "box-ticking" exercise, but "boxes" cannot be "ticked" unless this is substantially reflected in practice.
- Allowing organisations complete flexibility in how they evaluate their own data risks via Privacy Management Plans will lead to a mishmash of methods and approaches that will make comparison and enforcement difficult.
- **Good-faith organisations benefit from existing accountability rules in that they are not only risk-based and proportionate, but also prescriptive**: this provides them with clear requirements to fulfil. **On the contrary, scrapping these requirements will give extra lee-way that bad-faith actors will take advantage of.**
- Many companies would need to comply with the EU GDPR accountability framework and the UK Privacy Management Programme, thus increasing their regulatory burden rather than reducing it.

Furthermore, and in relation to some specific proposals:

- **Removing the requirement for an independent DPO will reduce the need to appoint an expert with sufficient autonomy and resources to ensure that people's personal data are protected effectively.** Privacy officers will focus on following orders rather than promoting compliance or positive change in their organisations.
- **Records, DPIAs and other assessments act as a filter to consider and alleviate the negative impacts of high-risk processing.** Removing prescriptive requirements for DPIAs and ROPAs gives discretion to the organisations that have a vested interest in giving themselves a good mark on their risk assessment, or their records;
- **Removing prior-consultation requirements effectively admits that high-risk processing operations will be allowed by default.**

5. INDEPENDENT OVERSIGHT

Independent Supervisory Authorities operate as one of the critical actors in the field of privacy regulation, safeguarding civil liberties and individuals' rights by monitoring and enforcing compliance with data protection norms.

Their independence from the political domain becomes pivotal: as data processing is now ever-present and increasingly complex for individuals to understand, independent supervision is indispensable for the effective protection of the individuals' rights and freedoms regarding the processing of their personal data.

Instead, Data: a new direction argues in favour of aligning the ICO regulatory function to other regulatory agencies, omitting that those agencies are not watchdogs and do not act independently from the Government.

In the following section, we explain how the UK Data Reform Bill would undermine the independence of the ICO, and introduce burdensome requirements that will further hinder the effective enforcement of data protection law.

5.1 Undermining independent oversight

The UK GDPR provides the Information Commissioner's Office (ICO)

"monitor and enforce the application of this Regulation [the UK GDPR]"
"shall act with complete independence in performing its tasks and exercising its powers" and "remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody".

Instead, the UK Data Reform Bill intends

- To introduce a duty "to ensure that the regulator is required to have regard to competition, growth and innovation." which would be "Sitting below the principal objective" of the ICO, as well as "a duty to ensure the ICO also has regard to public safety" (Q5.2.4, 5.2.5).
- "To introduce a power for the DCMS Secretary of State to prepare a statement of strategic priorities (SSP) for the ICO to have regard to when discharging its data protection functions", including "its international priorities on data policy" (Q5.2.11)
- To remove the requirement "for Parliamentary approval and allow the Secretary of State for DCMS to amend the Information Commissioner's salary with approval from HM Treasury"(Q5.3.5).

- To introduce “a process for the Secretary of State to approve ICO codes of practice and statutory guidance” (Q5.5.3).

It is also worth mentioning that, contrary to the Government claim that the SSP would not have legally binding force, “the SSP will sit below the ICO’s primary objective and duties under the UK GDPR and the DPA 2018”. The ICO would also need to provide “A response to the government’s Statement of Strategic Priorities explaining what it proposes to do as a consequence of this statement” and to “report annually on activities taken, as set out in its response to the statement” (Q5.4.1, 5.4.2, 5.4.3, 5.4.4)

This would undermines the independence and effectiveness of the ICO from several perspectives:

- **The ICO would lose their independence:** they have to ask for permission to exercise some of their functions, they report directly to the Government as to how they are implementing the Secretary of State’s agenda, and they can be punished if they don’t follow orders.
- **The duty to enable “innovation and growth” will create conflicts where enforcement may have an adverse impact on the law-breakers.**
- **This framework overburdens the ICO and actively discourages them from exercising their function, at a time when we need an independent, stronger ICO more willing to intervene.** It makes it very difficult for the ICO to regulate and enforce the law (balancing conflicting duties such as with growth or public safety, impact assessments, bureaucracy etc…) but very easy for the ICO to ditch complaints (see above: right to lodge a complaint).

6. THE SUM OF ITS PARTS

We have seen as the UK Data Reform Bill would lead to a substantial erosion of the principle of legality, purpose limitation, and accountability. At the same time, individuals would be disempowered, and the Information Commissioner's Office would be put under Government control.

Any of these proposals significantly lowers the level of protection of personal data: it would undoubtedly cost the adequacy status, and impose significant compliance and administrative costs to any organisations in the UK that is offering services or products in the EU.

The sum of these proposals is even more concerning, as they would

- Create a brave new digital police state;
- Undermine innovation to favour the cronies and the law-breakers
- Create a hostile environment for victims of data-driven harms and discrimination.

We develop these points below.

6.1 Creating a brave new digital police state

The UK Data Reform Bill would give the Government the power to shape the regulatory environment to their likes, for instance by using secondary legislation to introduce

- new lawful grounds for processing;
- sweeping arbitrary derogations to the principle of purpose limitation;
- new international data transfers mechanisms.

In turn, **sharing data with law enforcement and other public authorities for detecting "crime and other safeguarding concerns" would become legal depending on Government's whims and regardless of the impact this may have on the lives of those being accused, investigated, or prosecuted.**

Plans to make online spying the default option will complement this new digital police state. Cookies will record everything we do, watch and read online, for the taking of the police and other public authorities.

At the same time, the UK Data Reform Bill would scrap the GDPR accountability requirements and replace them with empty, box-ticking exercises (privacy management programmes) where Government agencies will be allowed to choose what they need to prove, and give themselves a pat in the shoulder.

Finally, the UK Data Reform Bill will make sure that no one is able to challenge or question what the Government claim:

- When targeted with subject access requests, **the Government will be able to investigate the identity of the requester, the motives behind the request, and to reject it nonetheless**: those who dare to question the Government will be investigated instead;
- The Information Commissioner's Office would have to ask the Government for permission to exercise some of their functions. Further, t**he ICO will have to report directly to the Government as to how they are implementing the Secretary of State's agenda, and the Commissioner could see their salary curtailed if they don't follow orders.** Instead of overseeing or investigating the Government, the ICO new job will be to please their political masters.

6.2 Undermining innovation to favour the cronies and the law-breakers

Scrapping the balancing test will enable reckless uses of data, exposing individuals to harms and discrimination. At the same time, the UK Data Reform Bill would scrap robust accountability requirements and replace them with empty, box-ticking exercises where organisations will be allowed to choose what homework to do and give themselves a good mark. Organisations won't need to carry out risk assessments unless they want to, and they will be able to claim they are complying with the law, regardless of the substance of the assessments they have conducted.

In other words, and against the growing consensus that organisations should be more careful and considerate when deploying and using new technologies, the UK Data Reform Bill would exclude the need to consider the impact of these activities. Privacy management programmes will promote uncertainty and favour no one but the law-breakers and their lawyers.

Further, the new framework makes it very difficult for the ICO to regulate and enforce the law (balancing conflicting duties such as with growth or public safety, impact assessments, bureaucracy etc…) but very easy for the ICO to ditch complaints. Even if a complaint were to reach the ICO, the regulator would face burdensome procedural hurdles to regulate and enforce the law, and may even have to deny justice to the victims of abuses to "promote the growth and innovation" of the law breakers.

Finally, **the UK Data Reform Bill would also codify cronyism and corporate capture:** as Government powers are expanded and made arbitrary, bad-faith actors can easily trade favours with Ministers. The right lobbying, the right donation to the party in Government, or the right bribe will ensure that the laws are favourable and the eyes

of the ICO are closed. Indeed, the response to the consultation already mentions how respondents suggested that "further everyday business activities, such as human resources (HR) functions or fraud detection, should be added to the list". The original proposal in Data: a new direction also included "business innovation purposes that are aimed at improving services for customers".

6.3 Creating a hostile environment for victims of data-driven harms and discrimination

With the UK Data Reform Bill, everyone will have less rights, less choices, and less access to recourse when something goes wrong.

Proposals to **water down the right to human review reduces safeguards against unfair outcomes in automated decision-making, at a time when everyone agrees they should be strengthened.**

Proposals to **allow non-consensual online tracking or profiling seek to legalise unlawful and toxic practices**, such as discriminatory or predatory targeting, or micro-targeting for political disinformation.

Individuals seeking to exercise their rights would face a hostile environment, where they will be questioned about the motives of their requests, accused of being vexatious. Organisations are increasingly hostile to disclosing the information they hold about individuals. The UK Data Reform Bill would encroach and encourage law-breakers by giving them arbitrary powers and loopholes to refuse or charge for requests.

At the same time, the requirement to try resolving a complaint with the offender before complaining to the ICO will force victims of data abuses in undertaking privatised complaint procedures, where **offenders will have the opportunity to misrepresent facts and gaslight their victims into dropping their complaint.**

Finally, and even in the event that a complaint med it through this kafkaesque bureaucracy, **records and other accountability documentation will be hard to find or difficult to interpret.** On top of that, the ICO will be tasked with several burdensome requirements to either investigate or regulate, and they will need to balance any enforcement against the right of the law-breakers to "grow and innovate".