Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
Definitions, principles and lawful basis			
Definition of personal data	Personal data is defined as "*any information relating to an identified or identifiable natural person*". An "identifiable individual" is one who can be identified directly or indirectly. To determine whether an individual is indirectly identifiable, account should be taken of all the means 'reasonably likely' to be used either by the controller or by another person. Data which has been anonymised to the extent that it does not meet the standard of "personal data" does not fall within scope of the UK GDPR. Article 4 UK GDPR	The definition of personal data has been amended in an attempt to clarify the process for determining if information relates to an individual who is "identifiable". Information being processed will only be deemed to be information relating to an identifiable individual: (i) where the individual is identifiable by the controller or processor by reasonable means at the time of processing; or (ii) where the controller or processor knows, or ought reasonably to know, that another person will, or is likely to, obtain the information as a result of the processing and the individual will be, or is likely to be, identifiable by that	The definition of personal data is one that is often hotly debated. This amended definition limits the assessment in two ways. Firstly, it is limited to identification by the controller, processor or any third party who will likely receive the information, rather than (arguably) the world at large. Secondly, identification need only be by "reasonable means". This amendment is likely to be broadly welcomed, particularly by those organisations who seek to anonymise data. The current lack of clarity regarding whether data is truly anonymised often leads organisations to be overly cautious and treat almost all data as identifiable.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		person by reasonable means at the time of processing. Obtaining the information as a result of the processing includes "obtaining the information as a result of the controller or processor carrying out the processing without implementing appropriate technical and organisational measures to mitigate the risk of the information being obtained by persons with whom the controller or processor does not intend to share the information." Clause 1, Data Protection and Digital Information (No.2) Bill ("**DPDI**")	
Purpose limitation	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner which is incompatible with those purposes.	Whilst the concept of purpose limitation and incompatible purposes is maintained, specific provisions have been added to aid controllers when determining if a new purpose is compatible with	This amendment provides helpful clarification of, rather than significant change to, existing requirements.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	Certain factors to be taken into account when determining if a purpose is incompatible include the nature of the personal data and the context in which it was first collected. Articles 5-6 UK GDPR	the original purpose. Factors to be taken into account include: - the context in which the personal data was collected, including the relationship between the controller and data subject; - the nature of the personal data; and - the possible consequences of the intended processing. In addition, a specific list of purposes deemed to be compatible is provided which includes any processing carried out for the purposes of ensuring compliance with the lawful, fair and transparent requirement set out in Article 5(1) UK GDPR. Clause 6 and Annex 2 DPDI	
Legitimate interests	When relying on legitimate interests as a lawful basis, controllers must undertake a	A limited, exhaustive list of legitimate interests is set out in Annex 1. The	Legitimate interests is one of the more commonly relied on lawful bases and provides a useful "catch all" for controllers

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	three-part test known as a legitimate interests assessment or LIA. The third element of the test requires the controller to weigh up whether their interests in processing personal data outweigh the rights of data subjects. Uncertainty regarding the tipping point for success or failure of the balancing test leads to different outcome within similar organisations (potentially to the detriment of data subjects) and to some controllers to resort to relying on consent as an alternative lawful basis. Article 6(1)(f) UK GDPR	requirement to carry out the balancing test is removed for these processing purposes. Clause 5(9) sets out three non-exhaustive examples of processing that may be undertaken on the existing legitimate interests lawful basis: • Direct marketing. • Intra-group transmissions of personal data for internal administrative purposes. • Ensuring the security of network and information systems. However, unlike the recognised yet limited legitimate interests, the balancing test is still required in these instances. Legitimate commercial activity can be also be a legitimate interest, once again where processing is necessary and the	when other lawful bases are not appropriate. The limited, exhaustive list of interests which automatically "pass" the balancing test will be welcomed by controllers. The clarification also is welcome for those additional examples of activities considered legitimate interests subject to the balancing test.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		balancing test is carried out. Clause 5 and Annex 1 DPDI	
Processing for research purposes			
Definitions	Historical and scientific research purposes are not expressly defined in the body of the UK GDPR but addressed in the recitals. The concept of "scientific research" is introduced at Recital 159. Whilst a definition is not provided, the recital states that it should be interpreted broadly and lists a series of examples including "technological development and demonstration, fundamental research, applied research and privately funded research […] studies conducted in the public interest in the area of public health". The concept of "historical research" is addressed in a similar manner at Recital 160; again there is no definition but it is stated to include genealogical purposes.	Three new definitions have been added. Processing for the purposes of "scientific research" is defined as "processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded, including processing for the purposes of technological development or demonstration, fundamental research or applied research". The research may be carried out as a commercial or non-commercial activity. Research into public health will only be considered scientific research where	Amendment of the definitions from the recitals to the operative text of the UK GDPR provides greater clarity around what these terms mean.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	Recitals 159-160 UK GDPR	the study is conducted in the public interest. Processing for the purposes of "historical research" is defined as "including processing for the purposes of genealogical research". Processing for "statistical purposes" is defined as "processing for statistical surveys or for the production of statistical results where – (a) the information that results from the processing is aggregate data that is not personal data, and (b) neither that information, nor the personal data processed, is used in support of measures or decisions with respect to a particular individual". Clause 2 DPDI	

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
Consent	The usual UK GDPR standard of consent applies to processing for the purposes of scientific research. However, Recital 33 acknowledges that it is often not possible to fully identify scientific research purposes at the time of data collection and states that data subjects should effectively be allowed to provide a broader consent. Article 7 UK GDPR	The detail from Recital 33 has been moved to the operative text and expanded upon. Clause 3 DPDI	This broader consent mechanism where processing relates to scientific research will be welcome to those operating in this field. It will reduce uncertainty and concerns around the misuse of consent, as well as improving awareness of its potential as lawful basis.
Exemption to fair processing information requirement	Whilst there are a number of exemptions to the requirement to provide fair processing information, none apply specifically to processing of personal data for research purposes.	A new exemption has been inserted which applies where the controller intends to further process personal data for the purposes of scientific or historical research, archiving in the public interest or statistical purposes and providing the information would involve a disproportionate effort. Clause 9 DPDI	The change will ensure that research is not restricted in situations where re-contacting data subjects would constitute a disproportionate effort.
Data subject rights			
Threshold for refusing data subject rights requests amended from	The current threshold for refusing to comply with a request requires the controller to demonstrate	The current threshold has been amended from 'manifestly unfounded or	Dealing with data subject requests, particularly data subject access requests, can be particularly challenging for

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
'manifestly unfounded' to 'vexatious or excessive'	that the request is 'manifestly unfounded' or 'excessive'. These terms are not defined in the legislation but guidance suggests that a request may be manifestly unfounded if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purposes other than to cause disruption. Article 12 UK GDPR	excessive' to 'vexatious or excessive'. Each request should be assessed on an individual basis considering factors such as the relationship between the controller and data subject, the resources available the controller and the time lapse between requests. Examples of requests which will meet this threshold include those which are intended to cause distress, are not made in good faith or are an abuse of process. Clause 7 DPDI	organisations who deal with large numbers of requests. In recent years, we have seen an increasing number of instances where such rights are used as a "weapon". This amendment should make it easier for controllers to refuse certain requests and will be particularly welcomed.
Rights in relation to automated decision-making (ADM) and profiling	Data subjects have a right not to be subject to decisions based solely on automated decision-making, including profiling, which have legal or similarly significant effects, subject to certain exemptions. Where a decision is made, certain specified safeguards must be in place.	The provisions regarding automated decision-making have been replaced in their entirety. The definition of "solely automated" has been clarified to mean a decision where there is "no	Whilst these new provisions are framed as "conditions" for ADM, rather than a general prohibition, the effect is largely the same. The key change here is to limit the restrictions on ADM to those decisions which include special categories of personal data.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	Article 22 UK GDPR	meaningful human involvement". Instances of profiling will only be subject to the requirements under Article 22 where a significant decision has been made without meaningful human involvement. The restrictions now only apply where such a decision is based entirely or partly on special categories of personal data. In such circumstances, an automated decision may only be made if (i) the data subject has given consent; or (ii) the decision is necessary for a contract or required by law and a substantial public interest condition applies. In all cases, certain (arguably enhanced) safeguards must be in place including the right to obtain human intervention and contest decisions.	All organisations who use ADM functionality will need to review their processes to ensure that the relevant safeguards are in place.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		Clause 11 DPDI	
Data transfers			
Adequacy decisions	The UK GDPR currently mirrors the EU GDPR requirements for adequacy decision assessments. Article 45 UK GDPR	The regime for assessing the adequacy of third countries has been reformed and rebadged as a "data protection test" which focuses on risk-based decision-making and outcomes. The test will be met if the standard of data protection is "not materially lower" than that provided under UK law. The following factors are stated as being relevant: - respect for the rule of law and human rights; - existence and powers of a data protection authority; - arrangement for judicial or non-judicial redress; - rules regarding onwards transfers; - relevant international obligations; and	These amendments provide more flexibility for UK government when considering UK adequacy decisions. However, such flexibility could raise concerns within the EU regarding the UK's own adequate status, particularly if it is deemed that any onwards transfer from the UK is not subject to the same protections as those provided. This is a key area of change under the DPDI and will be monitored closely.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		- the constitution, traditions and culture. Clause 21 and Schedule 5 DPDI	
Alternative transfer mechanisms and proportionality of appropriate safeguards	In the absence of an adequacy decision, alternative transfers mechanisms such as the standard contractual clauses are available. The use of such transfer mechanisms is subject to the implementation of appropriate safeguards. Article 46 UK GDPR	The use of an alternative transfer mechanism remains subject to "appropriate safeguards". However, such safeguards are to be determined by reference to the "data protection test" (see above) and be based on the "reasonable and proportionate" assessment of the relevant controller or processor. Clause 21 and Schedule 5 DPDI	This is potentially a significant change which will allow transfer risk assessments to take into account proportionality and may provide organisations with options for a 'light touch' review e.g. where there is minimal or non-sensitive personal data.
Accountability			
General obligations	Controllers and processors are required to implement "appropriate technical and organisational security measures" to demonstrate compliance. Articles 24, 25 and 28 UK GDPR	References to "appropriate technical and organisational security measures" are replaced with references to "appropriate measures, including technical and organisational measures".	In practice, we expect this amendment to have little impact.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		Clause 12 DPDI	
Removal of requirement for UK representatives	Controllers and processors not established in the UK must appoint a UK representative in certain circumstances. Article 27 UK GDPR	This requirement has been removed. Clause 13 DPDI	This is likely to be a welcome development for those organisations with cross-border operations.
Replacing "data protection officers" with "senior responsible individuals"	Certain organisations are required to appoint a data protection officer (or "DPO"). The DPO has a prescribed list of tasks (and cannot be dismissed or penalised for performing those tasks), must be appointed on the basis of professional qualities, must be appropriated resourced and must directly report to the highest management level. Articles 37-39 UK GDPR	Removal of the requirement to designate a DPO. However, organisations will be required to appoint a senior responsible individual ("SRI") if they are a public body or carry out high-risk processing. The SRI will retain many of the characteristics of the DPO. The current drafting requires the SRI to "be part of" the organisation's senior management. The SRI may delegate his or her tasks to another person in which case such person should also be appropriately resourced and cannot be dismissed or	In practice, it is likely that existing DPOs will simply rebadge as the SRI. The requirement for the SRI to "be part of" the organisation's senior management could be problematic for existing external DPO appointments as the wording currently suggests that model is not permitted. Organisations should also carefully monitor any delegation of the SRI's responsibilities, noting in particular the protections which are extended to any person carrying out delegated tasks.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		penalised for performing those tasks. Clause 14 DPDI	
Replacing "records of processing activities" with "appropriate records of processing of personal data"	A requirement that controllers and processors maintain a "record of processing activities" (commonly known as a "ROPA") which contains a prescribed list of information. An exemption applies to organisations which employ less than 250 people unless the processing is likely to result in a risk to data subjects, processing is not occasional or involves special categories data/criminal offence data. Article 30 UK GDPR	Removal of the requirement to have and maintain a ROPA. The record-keeping obligations will be amended to apply to any controllers and processors, regardless of size, that carry out the processing of personal data which - taking into account the nature, scope, context and purposes of the processing - is likely to result in a high risk to the rights and freedoms of individuals. There was an exemption under Clause 15 of the original DPDI Bill for organisations which employ less than 250 people, unless the processing is likely to result in a risk to data subjects. This has been removed.	Whilst on first review this looks to be simply a change of name, the amended record-keeping requirement provides organisations with more flexibility to record their data inventory in a way that works for them. In deciding what is "appropriate", an organisation may take into account its own resources, the nature, scope, context and purposes of processing and risks for data subjects. However, as drafted, the information required to be maintained by a controller under the DPDI is more prescriptive. For example, it requires details of who the controller has shared, or intends to share, personal data with (rather than simply categories of recipients as required by the UK GDPR) and details of how long the controller intends to retain personal data (under the UK GDPR the requirement is to specify envisaged time limits for different categories of data, where possible). ~~The exemption is now slightly wider and therefore may benefit a greater number of organisations.~~

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		Clause 15 DPDI	The removal of the exemption will likely be welcomed by SMEs that employ more than 250 employees but do not undertake any data processing activities that could be considered high risk.
Replacing "data protection impact assessments" with "assessments of high risk processing".	A data protection impact assessments (or "DPIA") must be carried out where processing is likely to result in high risk to individuals. It is also good practice to complete one for other processing activities. If a DPIA results in identification of a data processing activity which poses high risks that cannot be mitigated, there is an obligation for prior consultation with the ICO prior to processing commencing. Articles 35-36 UK GDPR	Removal of the requirement to carry out a DPIA. However, organisations will be required to carry out an "assessment of high risk processing" which contains a summary of purposes of processing, assessment of necessity and risks to individuals and a description of how such risks will be mitigated. The Information Commissioner will be required to "produce and publish a document containing examples of types of processing which the Commissioner considers are likely to result in a high risk to the rights and freedoms of individuals"	The assessment of high-risk processing approach gives organisations more flexibility over the approach to and format of identifying and managing privacy risk, e.g. other existing processes could be leveraged. However, organisations also have the option to continue using existing DPIA processes (and are likely to do so if there is already an established process and organisational buy-in).

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		The mandatory requirement for prior consultation has been removed and replaced with a voluntary consultation process. Engagement in a voluntary consultation will be treated as a mitigating factor during any ICO investigation or enforcement action. Clause 17-18 DPDI	
Role of the ICO			
New statutory framework and overarching objective	No clear framework of strategic objectives and duties against which to prioritise its activities and resources evaluate its performance and be held accountable by its stakeholders. The ICO is obliged to fulfil a long list of tasks and functions, as set out in Article 57 of the UK GDPR, but without a strategic framework to guide its work.	New section inserted into the DPA 2018 setting out a statutory framework of objectives and duties to provide a stronger basis for the ICO to focus on transparent objectives which can be held accountable via Parliament. The section introduces a new principal objective for the ICO which seeks to ensure the ICO take a proportionate, risk-based	A clearer set of statutory strategic objectives and duties for the ICO will offer greater clarity and stability to the ICO's role and purpose, improve transparency, strengthen accountability in line with best practice of other regulators and provide some clarity to organisations as to how the ICO will operate.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		approach to its regulatory activities. The section introduces a duty to ensure the ICO also has regard to public safety. Clause 27 DPDI	
Growth, innovation and competition duties	No such express duties currently.	New section inserted into the DPA 2018 confirming that the government sees the ICO's remit as increasingly important for competition, innovation, and economic growth, and therefore intends to ensure that the regulator is required to have regard to the same. Clauses 27 DPDI.	The government has not made it expressly clear as to how these duties will be implemented or what their form will be. We imagine they will build on the existing regard the ICO have to the impact on economy when issuing fines etc., so not a wholesale change.
Statement of strategic priorities	Not a current requirement.	New section inserted into the DPA 2018 which introduces 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.	SSP will be a transparent way for the government to set out its priorities on data policy. The ICO's activity and objectives need to be more transparent, so that Parliament and the public can more easily hold the ICO to account as to whether it is meeting its responsibilities. Concerns have been

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		The SSP will sit below the ICO's primary objective and duties under the UK GDPR and the DPA 2018. Clause 27 DPDI.	raised about the impact on the ICO's independence; however, the ICO is not legally required to comply, but must respond to the SSP. The SSP will also be approved by the Parliament.
Governance model	The ICO is a 'corporation sole' meaning an individual person who represents an official position as a single legal entity. The powers and responsibilities of the ICO lie solely with the Information Commissioner, without a chair or an independent board created by statute. While the current model has been in place since the regulator's establishment in 1984, the ICO has grown significantly in size and importance.	New Schedule inserted into the DPA 2018 which moves away from the corporation sole structure and introduces a statutory board with a chair and chief executive. Schedule 13 DPDI (inserting new Schedule 12A to the DPA 2018).	This change will bring the ICO in line with other UK regulators such as Ofcom and the Financial Conduct Authority. Having powers and responsibilities spread across a board, rather than with one individual, should ensure greater independence, integrity and diversity.
Appointments process and salary	The Information Commissioner is appointed by Her Majesty by Letters Patent, following a recommendation from the Government based on merit, after a fair and open competition. Current legislation requires parliamentary approval to amend	New section inserted into the DPA 2018 mirroring the current Information Commissioner appointment process (by Her Majesty by Letters Patent) for the new chair role so in that respect, there is consistency with the existing legislation.	The appointment of the non-executive members via a public appointment process is in line with other regulators. Appointment of the chief executive by the board maintains the ICO's independence. Removal of parliamentary approval would bring the ICO in line with other regulators, which do not require salary approval from the House of Commons. Public corporation

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	the Information Commissioner's salary.	New section inserted into the DPA 2018 stating that the individual non-executive members of the ICO's future board and its chief executive officer role would be appointed by the DCMS Secretary of State via a public appointment process. The Government will not appoint the role of chief executive via a public appointment process as proposed in the consultation. Rather, this role will be appointed by the ICO's board in consultation with the DCMS Secretary of State. New section inserted into the DPA 2018 removing the requirement for parliamentary approval of the Information Commissioner's salary and stating that this will be determined by the Secretary of State.	salaries over £150,000 are already governed by HM Treasury's Guidance for approval of senior pay, which the Government believes provides sufficient safeguards to ensure value for money.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		Schedule 13 DPDI (inserting new Schedule 12A to the DPA 2018), paragraphs (3), (5), (10) and (11)	
Accountability and transparency	There is a lack of clarity around the ICO's strategic priorities in the current legislative framework, meaning that there are no clear objectives for the ICO to measure its performance against and report on.	New section inserted into the DPA 2018 which introduces legislative requirements for the ICO to report on its approach and performance (there is a lengthy list, including KPIs and its approach to exercising discretion concerning complaints). It will also need to report annually on its approach to enforcement, use of its powers (including the number of investigations undertaken and their nature, the enforcement powers used, the timeframes for all completed investigations and the outcome of the investigation process). Clause 38 DPDI (inserting new section 161A to DPA 2018).	Transparency is welcome, particularly given that it will enable organisations to understand the ICO's key areas of focus and approach to issues such as complaints handling, which has been inconsistent.

DAC BEACHCROFT

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
Codes of practice and guidance	The DPA 2018 requires the ICO to prepare codes of practice on four specified data processing activities, in order to provide practical guidance on compliance and outline best practice for organisations. The DPA 2018 requires the Information Commissioner to consult the DCMS Secretary of State, and any other individuals and organisations considered appropriate by the Commissioner, before preparing or amending three of the codes. The ICO is also required by law to publish statutory guidance on various areas, and under its general functions, the Information Commissioner has powers to develop and publish non-statutory guidance on processing activities that relate to data protection. Under its general functions, the Information Commissioner has powers to develop and publish non-statutory guidance on	**Requirement to carry out impact assessments** New section inserted into the DPA 2018 creating a statutory requirement for the ICO to undertake and publish impact assessments when developing codes of practice and guidance on complex or novel issues. This will apply to all codes of practice and statutory guidance unless exempt. Clause 30 DPDI (inserting new section 124C to DPA 2018). **Requirement to set up expert panels** New section inserted into the DPA 2018 requiring the ICO to set up expert panels to review a code of practice or guidance on complex or novel issues during its development.	**Requirement to carry out impact assessments** Whilst the ICO already carries out impact assessments for new codes of practice, this is only done as best practice and without statutory underpinning. This will ensure consistency when developing new projects and ensure that guidance is more effective and useful going forward. **Requirement to set up expert panels** This would build on existing best practice, for example, the expert panel set up by the ICO to support the age-appropriate design code. Government acknowledges the need to carry out a broad and transparent consultation process with an expert panel, and this will be built in. **Approval of codes of practice and complex or novel guidance** There will be valid concerns regarding the risk to the ICO's independence that this poses. To try and counteract this, the Secretary of State will be required to publish their rationale for approving or not approving a statutory code or statutory guidance produced by the ICO.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	processing activities that relate to data protection, but these can be hard to understand for SMEs.	Clause 30 DPDI (inserting new section 124B to DPA 2018). **Approval of codes of practice and complex or novel guidance** New section inserted into the DPA 2018 with requirements to carry out impact assessments and set up expert panels which would be accompanied by a power for the DCMS Secretary of State to approve codes of practice and complex or novel guidance, as a final safeguard. Clause 30 DPDI (inserting new section 124D to DPA 2018).	
Complaints process	Under the UK GDPR and the DPA 2018, there is currently no threshold to make a complaint to the ICO. The current legislation forces the ICO to allocate a significant amount of its resources to	New section inserted into the 2018 act putting in place a more efficient and effective model that would require a complainant to attempt to resolve their complaint directly with the relevant data controller before lodging a complaint	Many data protection complaints could be resolved more effectively between the complainant and relevant data controller or processor, prior to intervention by the ICO. In our experience the ICO is put to the task of considering complaints that are vexatious.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	handling data protection complaints.	with the ICO, alongside a requirement on data controllers to have a simple and transparent complaints-handling process in place to deal with data subject complaints. The ICO will have the ability to use its discretion to decide when and how to investigate complaints. This will include 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. Clause 39 DPDI	The ICO discretion will empower the ICO to exercise its discretion with confidence. However, this is not a complete win for controllers; in turn they will be required to consider and respond to data protection complaints lodged with them and have clear processes in place.
Enforcement powers			
Power to commission technical reports	When investigating infringements, the ICO has apparently faced challenges obtaining information from organisations regarding the	A new power has been introduced which permits the ICO to commission an independently-produced technical report to inform	We are concerned as to how these reports will be treated in terms of priority as against internal reports that are commissioned by the organisation from

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	technical and organisational measures that were in place at the time and the remedial measures applied. The perception is that this challenge in borne out of an attempt to hide internal failings and vulnerabilities identified as part of the organisation's own investigation (whether internal or by a third party specialist provider).	its investigations. This is akin to the power the Financial Conduct Authority currently has under the Financial Services and Markets Act 2000. The ICO will have the power to impose a monetary penalty notice where an organisation has failed to assist the "approved person" who is appointed to prepare the report. Clause 35 DPDI	specialist third party forensic investigators, for example. It was originally suggested that this power would be limited to particularly complex and technical investigations where there is a significant risk of harm or detriment to data subjects. However, such a limit has not been included in the DPDI, as currently drafted, and instead the Explanatory Notes refer to statutory guidance which will be published at a later date. We further note that the cost of having this report prepared is to be met by the organisation and not the ICO, and this may cause significant financial burden on companies that may already be meeting substantial costs following a cyber-incident, for example. Finally, we are unclear as to whether privilege will attach to reports required by the ICO and whether they may be disclosable to third parties who request copies of the same. Greater clarity as to how this power will operate in practice is required.
A power to compel witnesses to attend and answer questions at interview	Organisations have an existing duty to cooperate with the ICO but there has been a perceived reluctance of individuals to fully	A new power has been introduced which gives the ICO the power to compel a witness to attend and	Our experience to date has shown that organisations are typically at pains to assist the ICO with its investigations and we are yet to encounter an individual that

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
	cooperate with investigations, including a refusal to be interviewed. s. 63 DPA 2018	answer questions at interview. However, its use is limited to circumstances where the Commissioner suspects that a controller or processor has: (i) failed, or is failing, as described in s149(2) the DPA 2018, which includes non-compliance with chapter 2 of the UK GDPR (the Principles), data subject rights and obligations on controllers and processors, for example; or (ii) has committed, or is committing, an offence under the DPA 2018. Notably, Interview Notices may be imposed on current and former employees of a controller or processor, whether in a management function or otherwise. Limitations have been included as to what a person can be required to answer questions on, and there are exemptions which can be relied upon, such as where it might breach legal professional	refuses to engage. As such, we suspect that this power will not be widely relied upon and is likely to have limited application. In line with other regulators, such as the Financial Conduct Authority, it will need clear carve outs, such as for legal privilege and confidential information.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		privilege to answer questions. Clause 36 DPDI	
PECR			
Cookies	Consent for the use of cookies (and similar technologies) is required in all circumstances unless such use is strictly necessary. Regulation 6 PECR 2003	A new list of exemptions to the requirement to obtain consent is set out which includes the use of cookies (or similar technologies) for the purposes of: - installing necessary security updates; - ensuring user preferences are followed; - collecting information for statistical purposes about how the website/service is used with a view to making improvements. In order to rely on an exemption, the user must be given a "simple means of objecting". Clause 79 DPDI.	This will be welcome news to many businesses who wish to use analytics cookies in particular – as they either have a patchwork picture from lack of consents, or have been taking a risk based approach at risk of enforcement action. It remains to be seen how these changes will be operationalised and how the Government will discourage "scope creep" of the wide number of exceptions is has granted to the requirement for explicit consent.

DAC BEACHCROFT

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
Direct marketing	Soft opt in is not available for non-commercial organisations. Regulation 22 PECR 2003 (is required to be marketing of "products and services" so can only apply to commercial marketing, as clarified by ICO guidance) Political campaigning is subject to direct marketing rules. s. 122(5) DPA 2018 (captured under "advertising or marketing material", as clarified by ICO guidance)	Under the DPDI the soft opt in is extended to non-commercial organisations. The secretary of state has also been granted with the right to issue regulations to permit direct marketing for "the purposes of democratic engagement". Clauses 81-84 DPDI	The extension of the soft opt in will be welcome by non-commercial organisations but also "grey area" organisations such as market bodies etc., which previously may have had to take a risk based approach.
Nuisance calls	Currently in order to constitute a "call" (and therefore be subject to the PECR regime and enforcement action) a call needs to "connect". Regulation 2 PECR 2003 (definition of "call")	The DPDI extends the definition of a "call" to include "attempting to establish such a connection" i.e. simply making a call whether or not it connects. In addition, a new obligation has been introduced which places a duty on public electronic communications providers to notify the ICO in the event it becomes aware of	This is likely to increase the number of calls organisations (whether rogue traders or otherwise) will be considered to have made and such higher numbers will serve as an aggravating factor in the event of any deemed breach of PECR / nuisance call restrictions.

Theme	Current position in UK	Proposed position in Bill (as drafted)	Analysis
		any unlawful direct marketing. Clauses 80 and 85 DPDI.	
Enforcement	A breach of the PECR is currently subject to the enforcement regime under the DPA 1998 (to the extent not also a breach of UK GDPR) and is therefore capped at £500,000. Regulation 31 PECR 2003 (extends Part V of the DPA 1998 to PECR 2003)	The ICO will now have the same enforcement powers in respect of breach of the PECR as under UK GDPR / DPA 2018. Clause 86 DPDI.	Although it has always been a risk that breach of the PECR may also trigger a breach of the UK GDPR (and therefore the enforcement regime under it), this movement of the enforcement regime significantly increases the risk profile of activities governed by the PECR (cookies, marketing etc), particularly given that it continues to be an area of focus for the ICO.