noyb – European Center for Digital Rights
Goldschlagstraße 172/4/3/2
1140 Vienna
AUSTRIA

Vienna, 26.06.2023

URGENT: Freedom of Speech before Irish Data Protection Commission
(Amendment No 9 to the Courts and Civil Law (Miscellaneous Provisions) Bill 2022)

Dear Member of Parliament,

As you may be aware, the performance of the Irish Data Protection Commission (DPC) is of great importance, but has also received extensive criticism within Ireland, but also throughout Europe.

We were surprised to learn that, instead of reacting to criticism or implementing recommendations as laid out in the Report of the Joint Committee on Justice of July 2021, the Irish Government has now proposed a last-minute Amendment to the "Courts and Civil Law (Miscellaneous Provisions) Bill 2022", that would introduce a new Section 26A to the Data Protection Act. This new Section 26A would largely criminalise debates and criticism regarding the work and conduct of the DPC.

This unprecedented section could allow the DPC (as the only European Data Protection Authority) to declare almost any information on its daily operations to be confidential – making any free speech about these procedures a crime.

Public scrutiny is in many cases the last remaining form of democratic accountability of the DPC. Therefore, it is extremely concerning that the proposed amendment would (for the first time) legalise an already existing and largely illicit practice of the DPC to use alleged "confidentiality" of any information before it to undermine any public discussion on questionable practices or decisions.

For example, large parts of my own testimony before the Oireachtas Joint Committee on Justice on 27 April 2021 would not have been possible if Section 26A would have existed at the time.

Not only parties to procedures involving the DPC would run the risk of criminal prosecution when they criticise details of a procedure in public, but also journalists would be severely limited in their work.

We note that Meta[1] has previously approached EU law makers, regulators and courts to ensure that any procedure concerning their GDPR violations would be deemed "confidential" to ensure that big tech companies can continue to deny wrongdoing, even when subject to enforcement action. We are worried that the Amendment now follows Meta's demand for such a "gag order".

We are also concerned about the "last-minute" procedural when severely imitating the freedom of expression in a very delicate area. Section 26A was added to the "Courts and Civil Law (Miscellaneous Provisions) Bill 2022" at the very end of the legislative process. When the bill was first presented to the Dáil Éireann on 13 September 2022, no mention of such a massive limitation on the freedom of speech in such a delicate area was made. There was no public consultation, nor any submissions from affected parties. Now, only a week before you are asked to approve this bill a very substantial Amendment was introduced, that may not have received sufficient scrutiny by the Government.

Especially when fundamental rights are at stake, careful consideration must be given to opposing views and to the legislative process. A provision that gives a regulator the power to criminalize freedom of expression, warrants utmost care, due deliberation and input form relevant stakeholders.

As proposed, the amendment may not only violate the GDPR and conflict with the planned European GDPR Procedures Regulation, but it also severely limits the freedom of speech in violation of Irish and EU fundamental rights.

In addition, the Amendment will likely interfere with the DPC's existing duties to cooperate with other data protection authorities, who have to make documents of procedures freely available to the parties under other Member States' laws.

➔ ***We urge Members of the Oireachtas to vote against the last-minute Amendment 9 to the Courts and Civil Law (Miscellaneous Provisions) Bill 2022, introducing a new power of the DPC to issue "gag orders" under a new Section 26A of the Data Protection Act.***

Below, you will find a more detailed explanation as to the many problems we see with this amendment, to the extent that such an explanation was possible in the short period since the introduction of the Amendment last week. We remain available for any further questions and assistance.

Kind Regards,

Mag. Maximilian Schrems

[1] In procedures before the Austrian SA and via lobby groups that Meta is a member of in the public consultation on a new GDPR Procedures regulation, available via the European Commission website.

1. DPC's and Big Tech's strategy of abusing alleged "confidentiality" to undermine public debate would (for the first time in Europe) get legitimized by Section 26A

The DPC has a long history of extensively declaring all information and documents of any investigation "confidential" under the existing Section 26 of the Data Protection Act, even when the current law only applies to DPC personnel – not external parties.

In our cases the DPC has regularly declared mere legal arguments by Meta "confidential", even when it concerned submissions on information has to be published in the privacy policy of Meta under Article 13 or 14 GDPR and is therefore everything but "confidential".

When we cited from documents that we received by *noyb* under EU freedom of information law or the procedural law of other Member States (which all allow the free use of such documents) the DPC factually retaliated against *noyb* by unlawfully removing us from a complaint procedure without any legal basis in Irish or European law. In the same vein, the DPC threatened legal actions against *noyb* or its chairman Max Schrems for criticising the DPC on social media even though such criticisms was within done within the freedom of expression.

Equally, big tech companies like Meta or Google have tried to undermine GDPR procedures by declaring any email, submission or attachment "confidential", including information containing not even remotely commercially sensitive information and often times even publicly available.[2] *noyb* has repeatedly revived unfounded threads by big tech companies that were aimed at intimidating us and limit our public participation.

As a small non-profit such frivolous threats and legal challenges can easily paralyze the organization and mean than large party of donated funds must be diverted to legal costs.

Meta and the DPC have repeatedly taken (unsuccessful) action in litigation to remove *noyb* or the public from procedures, or resist its participation. In a recent case on the legal basis that Meta is using to process personal data of millions of Europeans under Article 6(1) GDPR, Meta has applied to the High Court to hear the case "in camera", without any oversight by the public or journalists – again on information that Meta is required to make public in its privacy policy under Article 13(1)(d) GDPR.

- ➔ ***There is already a highly problematic tendency by big tech and the DPC to use alleged confidentiality of information to remove parties and the public from the administration of justice.***
- ➔ ***The proposed Section 26A would, for the first time in the European Union, provide a legal basis for the highly problematic practice by the DPC and big tech of making extremely broad claims of "confidentiality".***
- ➔ ***Section 26A would likely embolden the DPC's and big tech's approach to simply declare any information that could lead to public reporting or scrutiny "confidential".***

[2] For example: Meta requested the DPC and the EDPB to remove user numbers from decisions as they were "confidential", which may at first seem legitimate – however, the same numbers were soon thereafter published by Meta itself.

2. Conflict with the right to freedom of speech

We are not aware of any situation where confidential information, such as trade secrets or other protected information, was exposed in procedures before the DPC. Such information is already protected by other laws and usually gets blackened by the DPC. Section 26A therefore seems to capture mere sharing of currently unprotected information.

In the last years, the DPC and certain big tech companies have engaged in a broad and extreme attempt to limit reporting and public discussion about merely legal exchanges or views in the public. This included for example Meta's or Google's arguments on why they think their processing is legal under the GDPR or the DPC's positions taken in draft decisions.

Such positions often determine the fundamental rights of millions of Irish and European users - which is why these companies try to avoid any public debate about their conduct. In our experience the concern of big tech is not the sharing of truly confidential information, but such claims are abused to simply manage public perception and reputation.

It is virtually impossible to criticise a pending procedures without also discussing facts about pending procedures. Section 26A is therefore a direct attempt to limit the freedom of expression by persons that have procedures before the DPC.

2.1. Freedom of expression is the default in a democratic society

Freedom of speech is a pillar of any democratic society. Article 40.6.1.i of the Irish Constitution, Article 10 of the European Convention on Human Rights and Article 11 of the Charter of Fundamental Rights grant the right to freedom of speech. Any limitation to the right to freedom of speech, must be necessary, not violate the essence of the right and be proportionate.

Section 26A is a direct limitation of the right to freedom of speech, as it criminalizes to speak about almost all aspects of pending DPC procedures. The provisions could be interpreted to also include just the fact that a certain step was taken by the DPC, or that a certain step took extremely long, as Section 26A broadly captures any "information".

2.2. Lack of need for protection & extremely broad application

While it is undisputed that certain information (such as trade secrets or intellectual property rights) warrants certain protection in legal procedures, Section 26A tries to make the entire decision process of a public tribunal and authority confidential.

Section 26A does not only protect specific documents, or specific sections of documents, but any "information" about and from a procedure – it is therefore extremely broad.

Section 26A seems to be at odds with the European legislators understanding of confidential information, which is aimed at only protecting information of actual secrecy (see e.g. Directive (EU) 2016/943).

Section 26A may therefore be interpreted as a provision covering information where there is no legitimate interest in protecting it. To the contrary, Article 6 of the European Convention on Human Rights and Article 47 of the Charter of Fundamental Rights (see below) generally requires that procedures before tribunals are public, setting a default rule that is opposed to Section 26A.

2.3. Disproportionate limitation of the freedom of expression & no balancing

Procedures before the DPC can take years, partly even decades.[3] The time period in which information has to be kept confidential is therefore in most cases extremely long. In fact, just speaking in public about how long certain steps took before the DPC acted could already be interpreted as a violation of the new Section 26A, as even durations of steps could constitute "information" about a procedure.

Freedom of speech that is effective only after a procedure is already decided, would defeat the purpose of such free speech. In the proposed Section 26A there seems to be no need to take the competing interest between public information, freedom of speech and other interests into account. Any information for almost any procedure may be considered "confidential".

The text of Section 26A also does not require to balance possible interests in confidentiality with the rights of others to exercise their freedom of speech. The provision does not seem to require a proportionality test as required under Article 52(1) of the Charter of Fundamental Rights and leaves the decision on the confidentiality of documents entirely to the DPC's discretion.

While confidential treatment of information by the employees of the Data Protection Authorities is accepted throughout the EU, we are not aware of any similar provision that would prohibit parties from just speaking about information obtained before any other Data Protection Authority in the European Union, or indeed other similar authorities in Ireland.

To the contrary, most European and Irish authorities are subject to extensive transparency obligations and Freedom of Information Laws – that the DPC is famously exempt from. The European Data Protection Board and other national Data Protection Authorities regularly provide the documents that Section 26A tries to make confidential under "freedom of information" laws to any (third) party that requests them. Ireland would depart from European standards even further when passing Section 26A.

- ➔ ***The proposed Section 26A is a direct limitation of the freedom of speech, exclusively applicable to parties before the Irish DPC. We are not aware of other similar Irish or EU authorities that would be able to criminalize speech that contains information on procedures.***
- ➔ ***Section 26A does not foresee a realistic way to challenge the abuse of the DPC's power to declare documents "confidential", leaving citizens with the risk of criminal prosecution when challenging the DPC's determinations.***
- ➔ ***Given the DPC's bold interpretation of its powers under existing legislation, Section 26A would likely lead to determinations that violate the freedom of speech under Article 40.6.1.i of the Irish Constitution and Article 11 of the Charter of Fundamental Rights.***

[3] See e.g. a complaint by Max Schrems on Facebook's EU-US data transfers that was filed in 2013 and is still not decided by the DPC more than ten years later, despite two judgments by the CJEU.

3. Conflict with the right to a fair trial under Article 6 ECHR

Article 6 of the European Convention on Human Rights (ECHR) establishes that procedures before a tribunal (like the DPC) are by default public. Equally, Articles 41 and 47 of the Charter of Fundamental Rights ensure that parties have full access to any file of their cases and that procedures before tribunals are held in public. We are not aware of any European Data Protection Authority where procedures are declared "confidential" to the extent that Section 26A foresees.

In line with this established standard in any modern democracy, Article 34.1 of the Irish Constitution establishes that justice is administered in public. While this only covers Courts and not tribunal, exactly the same logic applies to any independent decision maker. Public scrutiny shall ensure that independent decision makers are at least accountable to the public.

It seems that it is exactly the influence of public debate and reporting that limits the options for abuse by decision makers, which the DPC and big tech firms now try to criminalize.

The DPC and some big tech firms have recently tried to pervert these long-established principles by claiming that public scrutiny would be an "undue influence" on procedures.[4]

Especially, the proposed Section 26A(5)(c) makes clear that the provision is explicitly aimed to prohibit the use of any information that could "*prejudice the effectiveness of the performance of a relevant function*". In the previous interpretation by the DPC, this was especially used to try to prohibit any public criticisms of decisions or procedures, such as the fact that the Irish DPC structurally departed from European guidelines or removed evidence from a procedure.

The DPC took the view that even just pointing out that they depart from EU law, EU guidelines or their duties to decide would form "undue influence" on the procedure. Equally, big tech firms, claimed that public debates over their GDPR violations or just open letters to EU regulators on highly problematic procedures (like the removal of evidence from the case files by the DPC) would amount to such "undue influence" on a procedure.

However, the very reason for a decision-making process to be done as public as possible is that the public can have a watchful eye on questionable or problematic actions by decision makers. Unproblematic actions hardly get public attention and even if unfair criticism would arise, the DPC would not have any reason to depart from an otherwise accurate path. However, when the DPC is faced with legitimate criticism by citizens or the media, the solution does not lie in criminalizing this criticism, but in taking the criticism on board and improving the DPC's performance.

If the proposed wording of Section 26A would pass, the narrative of the DPC and big tech firms that any public accountably is an "unfair" influence would be further emboldened and could be seen as legitimized by the Irish legislature.

- ➔ ***Section 26A establishes a principle of confidentiality, which is contrary to the default principle of administering justice in public under Article 6 ECHR, Article 37.1 of the Irish Constitution and Articles 41 and 47 of the Charter of Fundamental Rights.***
- ➔ ***When the DPC and big tech is faced with regular criticism by citizens, the solution does not lie in criminalizing this criticism.***

[4] Recent submissions of Meta Ireland Limited before the High Court, which are themselves subject to discussions about confidentiality and can therefore not be cited here.

4. No realistic way to challenge overly broad claims of confidentiality by the DPC or big tech

Given that the DPC and big tech have a history of extremely broad claims of confidentially – even when no provision like Section 26A existed, it is likely that the DPC and big tech will make even broader claims under the new provision, with no oversight.

It therefore seems especially problematic that Section 26A does not explicitly foresee a mechanism to challenge an inaccurate classification by the DPC. There may be an option to bring a Judicial Review - but this would usually cost up to € 100.000 and take years to be decided.

In practice, the DPC would be free to make excessive claims under Section 26A. Given the fact that the DPC made such claims even when there was no legal basis as proposed under Section 26A, it is highly likely that the DPC would make excessive use of Section 26A.

- ➔ ***Citizens and civil society would be unable to question the DPC's practices, if they would have to stay silent about the exact procedures they may wish to criticise.***
- ➔ ***There seems to be no realistic path to challenge overly broad claims by the DPC and big tech. Any challenge to an overly broad interpretation of Section 26A would likely require a Judicial Review. Such legal procedures between the DPC, big tech and average citizens, would likely bankrupt citizens, given the current costs[5] in GDPR litigation in Ireland.***

5. Limitation on journalism and public scrutiny

The DPC is the regulator for many of the most relevant "big tech" companies in Europe. This generates additional public interest in pending procedures, fines and appeals. Cases before the DPC usually attract the worldwide media, which clearly increases the stakes for everyone involved.

The Irish DPC has a long history of problematic decisions, conducting strange procedures and a lack of cooperation with its European counterparts as well as a lack of even minimum transparency towards them and the public. This led to extensive criticism by citizens, European counterparts and the European and Irish legislator. As GDPR procedures are often very technical and hard to understand, detailed background information is crucial to to make third parties understand these decisions, allowing public debate or criticism of such decisions.

It is virtually impossible to report or discuss such cases and problems in procedures (e.g. that the DPC regularly departs from European guidelines or that big tech companies have questionable meetings with the DPC) without also using information that concerns these pending procedures. In an environment where big tech aggressively threatens media outlets to litigate if they cannot proof that their reporting is accurate, journalists are extremely dependent on having access to verifiable information and documents.

It is crucial that such issues are made public in a timely and accurate way. As currently drafted, Section 26A would likely be used to undermine such reporting and public accountability.

[5] Most procedures noyb is engaged with have estimated costs of € 100.000 and upwards.

➔ ***The procedures before the DPC attract international attention, but also consistent and wide spread criticism.***

➔ ***Journalists need access to verifiable information to report about the consequences for big tech firms, but also for millions of their users.***

➔ ***Section 26A would severely limit the work of journalists.***

6. Conflict with existing duties of Big Tech and the DPC under the GDPR

The DPC has a long-standing history of less-than-ideal cooperation with data protection authorities in other Member States. These authorities regularly report that the DPC does not provide documents, does not respond to requests and even withholds documents upon request – despite a duty to cooperate under Article 60 to 66 GDPR.

The DPC regularly cites "Irish law" as a reason that it cannot fully cooperate with its European counterparts, even when Irish law experts explain to us that such limitations do not exist - until now.

Section 21A does not exempt other EU supervisory authorities from its application when cooperating with the DPC under Article 60 to 66 GDPR. The law would allow to declare documents confidential towards other SAs, which would make them potentially subject to Irish criminal law.

If Section 21A is passed, it would very likely create a situation where Irish law would fundamentally depart from the laws and procedures before most other SAs – creating even more cause for friction than today. Taking into account the principle of supremacy of EU law, the duty to cooperate under the GDPR would clearly have precedence over any limitation in Section 26A. It is however not unlikely that the DPC would further use this provision as a reason to limit cooperation.

Consequent, it seems unwise to pass an Irish provision that cannot be complied with when the DPC operates in cross-country procedures and that is even likely to be declared inapplicable by the CJEU following a request for preliminary ruling under Article 267 TFEU.

In addition, transparency is at the core of the GDPR. Article 5(1), as well as many other provisions like Articles 13 to 15 GDPR require companies to be utmost transparent with users. It is counterintuitive that the GDPR requires transparency, but Irish procedural provisions would suddenly require confidentiality once a GDPR claim comes before the DPC.

➔ ***We are concerned that Section 26A would create further conflicts with the DPC's duties under Articles 60 to 66 GDPR.***

➔ ***Given the DPC's history of withholding documents from other SAs, we are concerned that Section 26A would serve as another basis for the DPC to limit European cooperation.***

➔ ***The GDPR requires utmost transparency of companies, it would be counterintuitive that the opposite would apply as soon as a user brings a GDPR claim before the DPC.***

7. Conflict with other EU legislation

Article 54(2) GDPR seems to (ultimately) deal with matters of confidentiality in GDPR procedures, insofar as it stipulates a duty of secrecy on the staff of any SA – but does not extend that duty to parties before an SA. It seems unclear if the Irish legislator has the power to extend Article 54(2) GDPR to any third party.

We also note that the EU has recently announced a GDPR Procedures Regulation which is meant to regulate procedural matters of cross-border procedures, such as confidentially of documents or procedures as such. It seems premature to now quickly pass an Irish provision on the matter, when a European clarification is in the making. It is to be expected that the upcoming GDPR Procedures Regulation will regulate the matter of confidentially different than Section 26A. Again, this will lead to potential inapplicability of the Irish provision and scrutiny be the CJEU.

We would also like to point to a proposed EU legislative act on so-called "SLAPP" litigation (which is intended to limit litigation against non-profits and political participation) and to the recently passed Whistleblower Directive. Section 26A seems to conflict with this approach, at least in spirit, as it would further reduce public participation and even criminalize freedom of expression.

➔ ***It seems questionable if Section 26A can extend a duty of secrecy in Article 54(2) GDPR to third parties, when this is not foreseen in EU law.***

➔ ***The proposed Section 26A may conflict with the upcoming GDPR Procedures Regulation and with the spirit of other EU legislation, such as upcoming Anti-SLAPP-Legislation and the Whistleblower Directive.***

8. Quality of the proposed amendment

We note that Section 26A also seems to suffer from poor legislative drafting. We would like to highlight the following issues as examples:

The exemptions to use information in Section 26A(2) seem to be rather generic and broad. There may be hundreds or thousands of laws in various countries that "require" or "permit" the use of information:

- Obviously, Article 11 of the Charta of Fundamental Rights "permits" the freedom of expression. A reading that would reconcile Section 26A with Article 11 would clearly require that disclosures could be made under this provision, as far as such disclosures are necessary to exercise the freedom of expression. However, it is questionable if this would also be the view of the DPC, as it has previously used Section 26 to also interfere with the freedom of expression.
- In many countries stock companies have duties to inform their stock holders about ongoing legal procedures, especially if they could lead to substantial fines. In many cases such requirements would trump Section 26A for larger commercial players.
- Procedural laws in many countries permit or even require to provide "confidential" (or even illegally acquired) information as evidence in procedures. The legal traditions within the European Union are vastly different and lead to problematic results.

Overall, this clause allows for many reasonable interpretations that could defeat the very purpose of Section 26A, as intended by the DPC. In addition, such exemptions may lead to situations where one party to the procedure could talk about details more freely than others.

The term "relevant person" seems to be very broad and could e.g. also include other authorities in Ireland and in other EU Member States, journalists, legal representatives like lawyers or other parties, that may get information by the DPC to perform their professional conduct. The DPC would be enabled to directly interfere with their duties and rights under Irish and foreign laws.

Equally the term "disclose" is very broad and could be interpreted to even include the sharing of information with a legal representative, an organization operating under Article 80 GDPR or a close friend or family member, that a complainant may want to ask for help.

It is unclear how this provision would be able to cover disclosures that occur outside of Ireland, as it seems that the DPC would lack jurisdiction.

- ➔ ***Much of the wording for the provision seems to be very broad and could (in the light of the already extensive interpretation of the existing Section 26 by the DPC) go far beyond any legitimate protection of truly confidential information.***
- ➔ ***On the other hand, the broad exemption whenever a person is "required or permitted" by (any) law to use such information could render Section 26A largely meaningless.***
- ➔ ***There may be unequal treatment of the parties, as some may be able to rely on an exemption under Section 26A(2), while others are not.***

9. The DPC would gain enormous powers in the public discourse against the parties before it, but also against its European counterparts.

The DPC has a long history of very one-sided information on its work towards the public. This includes questionable and sometimes purely deceptive information about European procedures.

If Section 26A would be passed, the DPC may also gain enormous power in public discussions, as it can single handedly and selectively release information on procedures to the public, while at the same time criminalizing the parties before it when they voice their view on pending procedures.

This would lead to a very unequal situation when it comes to public information and public discussion, which would be highly problematic in a democratic society.

- ➔ ***Section 26A gives the DPC the option to drive a specific narrative in public reporting that would unduly benefit the public relations efforts of the DPC. This could lead to one-sided and even inaccurate information for the public.***

10. Section 26A would criminalize the only realistic form of accountability for the DPC and big tech

The DPC is a public body with exceptionally little oversight and accountability:

- Based on EU law the DPC is independent from the government.
- As the Report of the Joint Committee on Justice from July 2021 shows, the DPC is also hardly subject to legislative oversight. There is hardly any option for the legislative branch to require reasonable procedures by the DPC.
- While judicial oversight can play a role in many Member States, the costs of litigation in Ireland put judicial oversight out of reach for most citizens.
- The DPC also happens to be largely exempt from other democratic instruments, like the freedom of information act.

Consequently, public awareness and the role of the media remained one of the only forms of accountability for the DPC. Given the often problematic conduct of the DPC, this avenue was used by many complainants that were (rightfully) unhappy about the performance of the DPC.

Section 26A is now blocking this last avenue of accountability in most cases.

➔ ***The DPC is largely isolated from executive, legislative and judicial oversight.***

➔ ***Section 26A now blocks the main form of accountability in the form of public debate, media coverage and criticism by citizens.***

11. Unclear territorial jurisdiction

The amendment does not clarify the territorial jurisdiction of Section 26A. The Data Protection Act does not seem to clarify the geographic application either.

Especially in international cases, where the DPC is under a duty in Article 60 to 66 GDPR to cooperate, this may give rise to further friction, as the DPC has a long tradition to apply Irish law to international procedures and demand that other SAs also apply Irish law instead of their local procedural rules. The DPC previously also used alleged "confidentiality" rules to limit cooperation and exchanges with other SAs in Europe.

Given that the laws of most other Member States do not allow to declare average information "confidential" and instead require the sharing for documents with the parties (and often even third parties), the proposed Section 26A may be the basis of further disputes between the DPC and its European counterparts.

While Section 26A cannot logically apply outside of Ireland, this may put Irish parties to the procedure at a disadvantage, as parties in most other Member States would be free to speak about a case, while only Irish parties would be subject to Section 26A.

➔ ***We note that the DPC has a long tradition of forcing its understanding of Irish procedures onto other SAs in the Union and that Section 26A may be another situation where Irish law departs from European standards and therefore forms an obstacle to cooperation.***

- ➔ ***The lack of any clarification that Section 26A can (logically) only apply within Ireland may lead to further disputes.***
- ➔ ***Section 26A seems to be a structural disadvantage to Irish parties, while parties in other EU Member States will not be limited in their freedom of expression.***

12. Reasonable approach to truly confidential information

We fully agree that there is information that must legitimately be protected, such as trade secrets or information that concerns details of IT security or intellectual property rights. Protecting such information within the procedure is also a more proportionate approach than fully blackening it. However, this must be limited to such actual cases of protected information.

While Section 21A(5)(a) and to a certain extent (b) seem to be somewhat reasonable, especially the proposed Section 21A(5)(c) could be understood by the DPC to allow declaring almost any document 'confidential'. It is likely that big tech companies would urge the DPC to follow such an interpretation.

- ➔ ***There is an agreement that truly sensitive data, such as trade secrets must be protected in procedures. The DPC already has a practice to blacken them, which may be codified in law.***
- ➔ ***While Section 21A(5)(a) seems to be legitimate and a slightly revised version of Section 21(5)(b) could be understood as a reasonable definition of 'confidential information', we have great concerns about the possible interpretation of Section 21A(5)(c) by the DPC. We would advice to remove this subsection.***
- ➔ ***Finally, there would need to be a provision in Section 21A that would ensure that any limitations are proportionate and limited to the extent necessary. Typically, this would e.g. require to identify certain elements or paragraphs in a document to be treated as confidential rather than entire documents or procedures.***