American Chamber of Commerce Ireland

Office of the Data Protection Commissioner

Submission to the consultation on consent, profiling, personal data breach notifications and certification

31 March 2017

Consent

Under the European Union's General Data Protection Regulation, consent is one of the grounds for processing personal data. However, it is not the only ground and there is no suggestion that the GDPR expected that consent would be the first among equals. It needs to be recognised that any of the grounds in Article 6 may apply and that it is the responsibility of the data controller to identify the appropriate grounds.

Although the GDPR's definition of "consent" elaborates on the earlier definition from the Directive, it intentionally stops short of requiring "explicit" consent for ordinary personal data. This appears to indicate that GDPR intends for companies to have flexibility in how they obtain consent, consistent with the guidance set out in the relevant recitals.

In accordance with Recital 171 of the GDPR, pre-GDPR consents should continue to be valid if the manner in which the consent has been given is in line with the conditions of the GDPR. This is of course without prejudice to the application of Article 7(4) (requiring that performance of a contract (including the provision of a service) is not conditioned on consent to processing that is not necessary for the performance of the contract) and the requirements of Article 8(1) which addresses consent in the context of minors.

The American Chamber of Commerce Ireland is strongly of the view that the most important element of consent is empowering a user with all the necessary information available to them so as to make an informed choice with regard to their personal data use.

Question 1: How should freely given, specific, informed and unambiguous indication of the data subject's wishes be interpreted and implemented in practice?

The interpretation of the GDPR's consent provisions should align with the policy goals behind the concept of consent:

- Ensuring people have the information they need to make informed choices about their data.
- Ensuring people can use this information in deciding whether or not to give consent.

The Chamber is fully supportive of meaningful and effective measures to inform users of how their data is used and enable them to make choices in this regard. The Chamber would therefore suggest an engagement between data protection authorities and user interface professionals to discuss means by which users can be empowered to understand the uses of their data to which they have a choice to consent. These stakeholders can work together to avoid unnecessary service disruption in the context of requesting consent per Recital 32 of the GDPR.

Companies must have the flexibility to provide tailored processes depending on the circumstances and on constant technological developments. It is important that the act of providing consent does not become burdensome and disruptive to users as they interact with technology in every aspect of their personal lives and in their daily work. Regularly refreshing consent can lead to user fatigue, especially for services like email.

Question 2: What actions/activities on the part of an individual should be considered a statement or a clear affirmative action signifying agreement to processing of personal data?

- Companies should be enabled to focus on obtaining consent through a variety of means that are best suited to the nature of the service they provide and the needs of their customers.

- Industry and the Office of the Data Protection Commissioner should work together to articulate the different types of consent methods that are practical, manageable and implementable.

- The GDPR affords companies with an opportunity to modernise the way consent is presented/collected and to offer a positive and non-disruptive user experience. Modern consent models should follow a set of core principles to protect privacy, while promoting the free flow of information, innovation and economic growth.

Question 3: How can organisations demonstrate that consent has been obtained to the standard required by the GDPR?

- Recital 32 of the GDPR provides an indication as to the means by which consent can be captured.

- Other helpful methods to support consent might be providing users with a "privacy control panel" which could be a clear way for organisations to demonstrate that consent has been obtained or other privacy friendly user education tools. It would also provide the user with greater transparency and control on the data he/she shares. Affirmative opt-in methods might include signing a consent statement, a binary choice presented with equal prominence (i.e. "yes" and "no" where the yes is not highlighted by default), switching a technical setting away from the default or a type of "in product setting".

- It is important that companies are enabled to use innovative ways to obtain consent which do not cause disruption in the way in which users avail of services.

Question 4: What organisational systems and procedures will be required to prove consent was obtained?

- The use of systems and the procedures required will be specific to the context and the manner and medium through which the consent is obtained. The fact that a user activated or commenced a service at a particular date and time may in many instances be considered sufficient to demonstrate consent without prejudice to Article 7(4).

- Where there is a requirement to collect explicit consent or the use of data is not directly related to the service, such consents would be recorded in an easily retrievable form in a database with an appropriate timestamp to demonstrate consent.

Question 5: For how long should organisations retain proof that consent was lawfully obtained?

- The proof of consent should be retained for as long as the company relies on said consent as the legal basis for the processing of the data which was obtained.

- It needs to be recognised however that personal data which is collected using consent as the legal basis will very likely be subject to a new consent at a point in time in the future as a service develops. It would appear to be disproportionate to expect a data controller to retain a complete record of all such consents related to a service over time.

Question 6: What are the practical implications for organisations where consent is withdrawn by an individual?

Withdrawal of consent only implies termination of service where the consent to data processing is intrinsic to the service. Where use of personal data is not intrinsic to the service it is to be anticipated that a user can withdraw consent to such use but continue to be able to use the service. Consent withdrawal may also result in parts and features of a service ceasing to be available to a user.

Question 7: What are the consequences for the individual concerned when consent is withdrawn?

- If a service is conditioned solely on consent and that consent is withdrawn, individuals in effect are choosing to withdraw from use of the service. When a data subject no longer wishes his/her data to be processed for a particular purpose, it should be assumed that the data controller will no longer be able to process this data, and therefore no longer able to offer its services.

- Individuals should be able to withdraw consent at any time by terminating a service.

- If different processing activities have required different consents then withdrawal of some but not all consents may result in more limited services being made available.

- Where consent is withdrawn, there may be circumstances where the controller can still process the relevant data if it can rely on other pre-conditions to processing described in Article 6 of the GDPR.

Question 8: In respect of minors how should parental consent be collected in an online environment?

- Parental consent mechanisms should be developed by industry, in line with the GDPR which affords industry the opportunity to develop parental consent mechanisms via Codes of Conduct (Article 40(2)(g)). Depending on the service, there may be a particular mechanism that is most appropriate to the parents of minors using the service.

- The Article 29 Working Party and its successor, the European Data Protection Board, should allow industry to develop relevant Codes of Conduct to ensure any parental consent mechanism is appropriate to the particular technology or service being offered to minors.

- There are lessons to be learned from the Federal Trade Commission which has considerable experience in this area over a number of years. It is disproportionate to expect different compliance regimes, therefore a global approach will make it easier for data controllers to comply and ensure a higher standard of compliance.

Question 9: What are the practical challenges in an online environment in verifying the age of a minor to determine whether parental consent is required?

- The GDPR does not explicitly require controllers to "verify" age. Indeed, the term 'age verification' is very broad and can mean a number of things. For instance, it should be recognised that data controllers may adopt a number of different mechanisms to ensure compliance with Article 8, e.g. a data controller may include in its privacy policy, or terms, a clause indicating that, upon acceptance of the policy or terms, the data subject is confirming that he is of the appropriate age in his jurisdiction to use the service.

- The Chamber strongly believes that member states should act together and that data protection authorities should adopt and recommend a harmonised approach. Indeed, harmonisation is one of the key objectives of the GDPR. It provides clarity to both users and organisations. There is a broad consensus at international level that the parental age of consent should be set at the lower limit of 13. Child safety experts, digital policy experts, anti-bullying organizations, youth organisations and educational groups, among others, all support a lower parental consent age.

- A significant issue in this space is to ensure that age can be reasonably verified without placing an obligation on data controllers to collect information on all users. This would run contrary to the requirements of Article 11 of the GDPR and generally to the data minimisation requirements of the GDPR.

- It should also be noted that it is not possible for data controllers to verify the "parental responsibility" of a person giving consent as there is no practical means to collect and verify such documentation and even if it were possible there is no means to verify if a parent is still exercising parental responsibility.

- Additionally in most cases, a parent may not be using the same platform as a child and therefore a data controller has no direct means to reach them and seek consent. Where a parent is using the same platform as a child then collection of consent is easier to achieve.

- Another practical challenge relates to the position in relation to children where consent was validly collected from them prior to 25 May 2018 but who will be younger than the age set by a particular member state on 25 May 2018.

Question 10: In respect of special categories of personal data how should 'explicit' consent be interpreted?

Interpretation of 'explicit' consent under the GDPR should not depart from that under Directive 95/46/EC, which also requests explicit consent for processing involving special categories of data.

Question 11: What actions/activities on the part of an individual should be considered to indicate explicit consent?

- The Article 29 Working Party defined explicit consent as "all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. For example, explicit consent will be given when data subjects sign a consent form that clearly outlines why a data controller wishes to collect and further process personal data."

- Oral explicit consent is not excluded: "although explicit consent is traditionally in writing, be it on paper or in electronic form, (...) this is not necessary so it can also be given orally". However, providing proof of oral explicit consent might be challenging.

- The key issue is that the user has an opportunity to read and understand all relevant information in relation to personal data usage and is then presented with a choice as to consent.

- Despite the conditionality attaching to ordinary consent in Article 7, there is no doubt whatsoever that the standard for obtaining explicit consent remains higher than that for ordinary consent in the GDPR. Further guidance could helpfully address what precisely is understood to be the distinction.

Profiling

The ability to process data to extract new actionable insights is essential to a knowledge-based economy and a key to building the information society. The American Chamber of Commerce Ireland recognises the need to protect data subjects against the risks arising from some types of profiling that could produce serious harm, and to ensure they will be able to hold the data controller accountable for any negative consequences arising. It is notable that the GDPR does not restrict all profiling, and rather the focus is upon profiling which may produce legal effects or otherwise significantly affect data subjects.

Question 1: How will profiling activities currently undertaken in your industry be impacted by the requirements of the GDPR?

The new provisions of the GDPR should not be interpreted in a way that would limit profiling activities that comprise a core part of modern internet-based services, such as personalised music and movie streaming services, map and transport services, interest-based online advertising, and the industry business models based thereon. It should be confirmed with regard to ad-funded free online business models – which are fundamentally based on the premise that individuals agree to receive interest-based ads as part of the service – do not involve processing which produce legal effects or otherwise significantly affects users. Even in extreme cases where such online services might engage in such types of profiling producing legal effects or significantly affecting data subjects, it should be confirmed that the individual's right to object (where the processing is based on Article 6(1)(f) legitimate interests) to profiling is served by allowing him/her to delete her account without further requirements.

Question 2: How should the distinction between 'legal effects' and 'significant effects' be interpreted?

- There is no clarity provided in the GDPR regarding distinction between 'legal effects' and 'significant effects'. It is assumed that where for example monitoring of an employee's work performance based on a population profile led to a decision to terminate their employment that this would be both a significant and legal effect. Equally there would be situations where for example a negative credit decision based only on automated processes would produce a significant impact.

- In terms of legal effects, it can be expected that these would be more likely in the public sector where profiling might be used to identify potential cases of social welfare fraud or tax evasion which could have considerable legal effects for an individual.

- Decisions construed as having "legal effects" or "similarly significant effects" should be limited to those that would truly have an adverse impact on individuals' fundamental ability to function in society. By contrast, the mere ability to access an online service should be confirmed to not be a decision which has "legal effects" or "similarly significant effects". This is consistent with Recital 71, which describes "automatic refusal of an online credit application or e-recruiting practices without any human intervention". It should be clear that this "higher" category of automated decision making concerns only the "decisions" that a specific data controller makes regarding a data subject; it does not include the processing

activities of other data controllers or processors who merely process or provide data underlying the decision itself.

- It is clear that this is an area on which data controllers in both the public and private sector would benefit from greater guidance as to where data protection authorities consider there is the bigger impact.

Question 3: How should the requirement to vindicate the individual's right to obtain human intervention in the context of profiling be interpreted?

- A "human intervention" requirement is only practical for a small number of cases. Human intervention makes sense for specific decisions that could have significant implications for people when based on automation alone — for example, if a job applicant is rejected solely based on an automated analysis of her application.

- In contrast, human intervention is impractical for routine services based on people's interests (e.g. tailored online content) or for tackling fraudulent or abusive uses of online services. Those services use people's interests to deliver content and provide other services the consumer has asked for or agreed to. They also keep users safe and secure by preventing abuse of online platforms, and in any event such routine services would not create legal or similarly significant effects.

- Given the scale and speed at which data controllers need to make many decisions it is not possible to grant to an individual a permanent right to have all decisions in relation to them proactively subject to human intervention. That would be impossible to give effect to, compromising service providers' ability to provide customised and secure services which consumers seek. It is also clear that such practice is not envisaged by the GDPR.

- The concept of "human intervention" should generally be construed broadly to include the opportunity for data subjects to be presented with the factors that went into the controller's decision making process and contest these factors.

- The data controller can review the data subject's objections and render a final decision.

Question 4: How should the individual's right to give their point of view and contest a decision as regards profiling be given effect by a data controller?

- There should be no one specified mechanism by which an individual's request would be addressed as this will depend on the type of service offered, the type of decision making in question and the channels in which a data controller engages with an individual. The means should be easily accessible with an expectation of a response through that same means or otherwise.

- A data controller should be able to assess the legitimacy of the individual's request and that it is not unfounded. If the profiling is based on legitimate interests, the data controller must be able to receive the data subject's request and determine whether its legitimate interests are outweighed by the interests or fundamental rights and freedoms of the data subject. If

the data controller assesses that its interests outweigh the interests/rights of the data subject, it should be able to continue with the profiling activities. Data subjects should always have the option of terminating the service, without detriment, to ensure their interests are protected.

- Data controllers may also be encouraged to provide data subjects with control or preference management tools that allow the data subject to modify what criteria is used to inform the data controller's profiling activities, to the extent that such profiling produces legal or similarly significant effects.

Question 5: What are the implications for organisations in implementing measures to respect the individual's right to specific information, to obtain human intervention, and to express their view and contest a decision?

- The American Chamber of Commerce Ireland does not consider that there are many significant practical implications facing its member companies from providing a means for an individual to obtain information and express their view.

- The practical issues that will arise are more related to the circumstances in which an individual can correctly assert their right. It is worthwhile to note however that these measures may prove particularly burdensome for small and medium enterprises, who may not have the resources to provide human review/intervention for decisions that qualify as producing "legal effects" or that "similarly significantly affect" data subjects. Similarly, it will be burdensome for SMEs to build systems or portals to take in objections by data subjects; review those objections; and communicate replies to data subjects.

Question 6: What types of public interest reasons would justify profiling?

The security of networks and the prevention of fraud are legitimate public interests as there is a need in the interests of all users to take steps to prevent bad actors from compromising security or perpetrating fraud which will ultimately have an impact on all individuals.

Question 7: Are there limits to profiling? Should certain activities and/or information be excluded from profiling?

- The GDPR's definition of profiling appropriately includes basic online business activities such as segmenting customers by interest or geography in order to provide helpful tips or relevant advertisements. Those advertisements are what support a fee-free internet for people of all backgrounds. This category of profiling is often referred to as "normal" profiling.

- The GDPR rightfully acknowledges that many businesses can't offer the core services people rely on without normal profiling such as interest-based advertising. However, such "normal" profiling should be confirmed not to produce legal or similarly significant effects. Data subjects may always avoid such profiling by opting out of the service, without detriment.

- There may be a natural tendency to identify certain sensitive categories of data and indicate that they should not be subject to profiling and this may indeed be a reasonable general

guidance to be given. However, it needs to be noted that the requirement in the GDPR only relates to profiling which has significant or legal effects on the individual.

- To provide their core services, sometimes businesses use automation to process some basic personal information e.g. an online retailer may analyse data on how people's spending patterns vary during major holidays in order to make decisions about inventory and staffing. These kinds of activities fall under legitimate interests. They are far different from activities that pose risk or significant impact to consumers, such as the automatic refusal of an online credit application.

- Processing basic personal data in low risk ways — such as generally categorising people for expected advertising purposes — should not be subject to higher standards. It's logical to assume that this is the GDPR's intention given that direct marketing already constitutes a legitimate interest (consideration 47) and requires even more granular data than the low risk activities described above.

Question 8: Where profiling involves special categories of data, what additional protections should apply to safeguard the individual's rights and freedoms and legitimate interests?

- According to Article 22, profiling shall not be based on special categories of data unless the data subject has provided explicit consent or where the processing is necessary for reasons of substantial public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place. Such measures could include for example anonymization or pseudonymization.

- There is a need for guidance for de-identification generally. The Office of the Data Protection Commissioner should therefore provide guidance in the form of international standards like ISO/IEC DIS 19944).

Personal Data Breach Notifications

The American Chamber of Commerce Ireland is of the view that governments should facilitate wider adoption of cyber security best practice and ensure that cyber resilience is built into all technology and training from the bottom up, rather than relying on a reactive approach to solving problems

Question 1: What are anticipated to be the practical implications for organisations in complying with the personal data breach notification provisions of the GDPR?

- The American Chamber of Commerce Ireland generally welcomes the materiality thresholds continued in the GDPR of risk and high risk for notifying supervisory authorities and affected individuals respectively.

- There are several steps to responding to a potential or suspected incident which may ultimately be determined to be a "personal data breach." At a high level, the data breach notification provisions of the GDPR should incentivise organisations to invest in a high degree of data protection. However, the precise timing specified for the notification requirements should not be used as a means to punish organisations or dis-incentivise responsible investigation and incident response; rather, data protection authorities should encourage entities to make partial, phased notifications, where that is the appropriate and obvious course, without regulatory penalties so as to ensure the protection of data subjects.

- The requirement that a data controller reports to a data protection authority the "consequences of the personal data breach," as set forth in Article 33(3)(c), will present a particular challenge as anticipating potential outcomes is an exercise in prognostication balanced by risk management. In lieu of speculation, this requirement should be interpreted to require data controllers to provide indications to the data protection authority as to how to reduce or mitigate potential impacts and harms resulting from a personal data breach.

- Notification, in a high risk situation, to data subjects presents a vital channel for those most impacted by a data breach to take actions to protect their rights and freedoms. Pragmatically applying this high risk standard will allow organisations to responsibly consider risks and ensure data subjects are not overwhelmed by data breach notifications that lack actionable information and are not likely to present real risk. This will result in breach notification fatigue.

- There is also a need for data protection authorities to confirm the position in relation to data breaches which may have intra-EU cross border implications. It should be possible for data controllers to reasonably assume that reporting a data breach to their lead supervisory authority meets the reporting obligations within Article 33. There should be no expectation that a data controller with a main establishment in one member state should have to make multiple reports and potentially face multiple investigations. Any such expectation would not be consistent with the principles of co-operation and consistency in Chapter VII of GDPR. Where co-operation is required in an investigation between Data Protection Authorities this

should take place within the context of the co-operation arrangements specified in the Regulation.

- Many businesses, especially SMEs still lack basic knowledge of the GDPR and the regulatory requirements that it will place on their business. The regulator should focus on ensuring that businesses understand their responsibilities in this regard, including the thresholds that trigger notification to the regulator and, separately, notifications to data subjects.

- There may also be a lack of knowledge within organisations regarding who to contact in the event of a breach and how employees should submit the relevant information. Organisations may need to undertake significant internal training and communications programmes.

- Flexibility in this area is required given the different structures which exist in every organisation.

Question 2: How should "risk to the rights and freedoms of natural persons" be interpreted?

While Recital 85 sets forth certain examples of what "risks to the rights and freedoms of natural persons" could entail, data protection authorities will no doubt wish to be less prescriptive about such risks. As society continues to evolve and organisations are charged with evaluating these risks in light of a data breach, certain risks may be inordinately challenging to rigorously pre-define. Further discussion should therefore be encouraged and the development of informal and interpretive guidance as data protection authorities and data controllers alike manage reporting requirements under the Regulation.

Question 3: How should "high risk to the rights and freedoms of natural persons" be interpreted?

As set forth in Recital 86, circumstances of "high risk" may exist where there is "immediate risk of damage" or the individual may have the need to "implement appropriate measures against continuing or similar" data breaches. Organisations should be permitted to conduct a reasonable "risk of harm" analysis to determine the risks in context of the manner in which data was collected.

Question 4: What are the circumstances in which a data controller should be considered to have "become aware" of the data breach?

- Data controllers, particularly in large and complex organisations, must retain the discretion to conduct an investigation to determine when a personal data breach has occurred. The rights and freedoms of data subjects would be unnecessarily impacted should premature notification of potential or suspected data breaches take place.

- Data controllers must not be considered "aware" of a data breach merely because such an incident is suspected; nor should the 72-hour requirement begin to run merely due to public reporting of a potential incident impacting the data controller, including by third parties.

- A data controller may appropriately be considered "aware" of a data breach upon:

  - Actual knowledge or confirmation of such a breach by responsible officers within a data controller. One report by a concerned customer, without supporting evidence, does not automatically make a data controller aware. There needs to be a concept of a threshold of information before which responsible officers could be reasonably expected to be engaged;

  - Where a personal data breach is suspected, at the conclusion of a reasonable and appropriate investigation under the circumstances and the suspicion is confirmed.

- While there should not be a rush to judgment, data protection teams should be involved at each step of such an investigation so as to ensure timely awareness is developed.

Question 5: In what circumstances would it not be feasible for a data controller to report a data breach to a data protection authority within 72 hours?

- In the event that there is a serious security breach which gives rise to a real risk of serious harm, the data protection authority and consumers should be notified as soon as practicable. The goal of any notification guidance should be the protection of the rights and legitimate interests of the data subjects, goals that are supported by notice so data subjects can react individually, and also by providing sufficient time for a serious breach to be identified and mitigated.

- The American Chamber of Commerce Ireland supports requirements of mandatory notification when data breaches occur. These requirements should be calibrated to provide timely, meaningful information.

- Where a law enforcement or national security agency is pursuing an investigation or requests or mandates the data controller to keep a security breach secret or requests or mandates non-disclosure, then it may not be feasible to notify a supervisory authority within 72 hours.

- Data breach notifications which are issued in a short time frame risk giving supervisory authorities, and ultimately data subjects, inaccurate or incomplete information.

- Given the often multinational nature of data security incidents, there can be complex and conflicting mandatory reporting and non-disclosure obligations; and the needs or requests of law enforcement and national security agencies in various jurisdictions can also complicate such efforts. It is often not possible, in the days immediately following the confirmation of a potential incident, to confirm that such an incident truly involved the

compromise of personal data in a reportable manner. For example it may not be possible for an organisation that has confirmed encrypted data was breached to determine within 72 hours whether such data included personal data or presents a risk of harm to data subjects. For this reason, the concept of "becoming aware of" needs to be interpreted pragmatically and carefully

Question 6: Where it is not possible for the data controller to provide all of the information required by way of notification to the data protection authority at the same time, what requirements should apply as regards the provision of such information "in phases without further delay"?

- It is vital that data controllers providing initial or interim notifications to a data protection authority of a data breach are afforded appropriate flexibility to report only that information relating to the breach which is confirmed or believed to be true. It should necessarily be expected that a data controller does not have all of the information required to provide a notification at the time of initial contact, and that the controller is conducting an active and often complex forensic investigation. Data protection authorities should permit data controllers during their initial contact to establish a reasonable timeline as to when further information will be provided to them. However, where it is clear that a data controller is treating a potential breach seriously and investigating it to the appropriate extent and with sufficient resources, it is vital that data protection authorities do not initiate investigations or pose unnecessary questions during this initial investigative period as active steps are likely underway to protect the rights and freedoms of data subjects. Where a data controller does not appear to be treating a matter seriously, then a data protection authority can be expected to launch an immediate investigation.

- In terms of what level of detail needs to be provided when informing the data protection authority of the data breach, Article 33 (3) describe the details of the information that should be provided. For security reasons, the notification of a personal data breach shouldn't provide too many details on the technical and organisational measures implemented by the data controller. For example in Article 33 (3)(d) a description of the mitigation measures can be released, but not all the technical details of the incident itself. This is also to protect confidentiality and IP rights and ultimately to reduce the risk of any enhanced security measures being compromised in the future.

Question 7: What type of measures should be considered sufficient to mitigate any adverse effects arising from a data breach?

- The data controller can mitigate adverse events, including as related to an ongoing potential breach, by remediating underlying issues using both temporary measures and ultimately more long term augmented security measures where appropriate.

- Measures that are made available by a data controller should be proportionate to the nature and risks associated with a personal data breach. Reasonable steps that align with requirements in other jurisdictions may include the establishment of a toll-free number for data subjects to contact the data controller for additional information so that they can take steps to protect themselves from any risks arising from the breach. However these services should not be required in response to all data breaches and should be selectively employed where necessary and appropriate. There is no one-size-fits-all measure; however measures that are aligned with international standards should be considered sufficient.

- Each data subject will necessarily have an individualised assessment of what potential adverse events may accrue from a data breach; as such, Article 33(3)(c) should be interpreted as an avenue for data controllers to provide information on how data subjects may mitigate adverse events.

Question 8: What type of measures should be considered sufficient to ensure that a high risk to the rights and freedoms of the individuals affected will not materialise?

- Data controllers should retain the ability to conduct risk assessments to determine whether a high risk to the rights and freedoms of individuals affected may materialise. Such assessments must necessarily consider the context in which the data was collected and the potential residual rights and expectations of the data subject.

- The degree of confidentiality with which personal data is expected to be kept may be considered as one factor in determining whether high risk exists; the sensitivity of personal data should not be considered alone. Data controllers should be encouraged to consider the context of the collection of data and associated permissions, and determinations regarding the risk of harm to data subjects must not be made in a vacuum abstracted from the facts.

Question 9: How should 'disproportionate effort' in notifying individuals be interpreted?

Proportionate effort to notify individuals may be made when the data controller has contact information for an individual readily available on internal systems. The data controller may make reasonable efforts – via a phone call, email or physical mail – to contact the individual in the event of a data breach. However, data controllers should not in all cases be required to affirmatively prove contact with each individual, and it should be considered disproportionate effort (and potentially prejudicing the further rights and freedoms of such persons) to require a data controller to undertake affirmative efforts to solicit or collect from the individual or third parties additional contact information for the purpose of notifying such individual of a data breach.

Question 10: In cases where notifying the individuals concerned would involve a disproportionate effort, what form of public communication or other similar measure to inform individuals would constitute an equally effective manner?

- Given the increasingly interconnected nature of the world, effective public communication can take a number of forms, and while certain forms of communication can be pre-judged to be effective, such determinations should not be prescriptive. Certain existing and broadly-available forms of communication – posting a notice to a data controller's webpage, issuing a press release to major services, potentially even a Twitter message – can serve to inform individuals in a more effective manner than expending disproportionate effort to notify on an individual basis. In many cases, such channels of communication, no doubt with consequent media attention, may be more than sufficient to put data subjects on notice.

- The appropriate communication to the data subject also depends on the relationship which exists with the data subject. Article 11 of the GDPR makes it clear that controllers should not have to take pro-active steps to aggregate additional personal information about data subjects for the sole purpose of complying with the GDPR.

Question 11: For how long should a data controller be required to retain documentation relating to data breaches?

Absent an independent legal responsibility to retain documentation, such as ongoing legal proceedings, data controllers should retain documentation in accordance with existing internal policies. Creating distinct retention requirements potentially increases the risk to data subjects (should their personal data be included in such documentation) and complexity that may disrupt existing, potentially mature processes. Where such records do not contain personal data, the controller can keep such records indefinitely. Litigation risk may also require that records including information about data subjects and the breach be kept for a reasonable period of time taking into account statutory limitation periods.

Certification

In order for compliance to be transferable across borders, the American Chamber of Commerce Ireland is strongly of the view that governments should ensure that legislation provides maximum flexibility and creates the least risk of conflict with other rules.

Question 1: What are the practical implications for organisations in seeking certification under the GDPR for:

- **Controller responsibilities?**
- **Data protection by design (Arts 24, 25)?**
- **Security requirements?**
- **Processor guarantees?**
- **Internation transfers?**

- ***Controller responsibilities***
  Controller responsibilities are relatively onerous under the GDPR and this must be reflected in the audit requirements for the certification. Appropriate data protection must be balanced with requirements to ensure "free movement of data" and respecting "data subject rights" (including ensuring security). This can have significant impacts on existing systems that were designed before these requirements came to the fore - and even greater impact for organisations that have personal data across multiple different systems.

- ***Data protection by design (Arts 24, 25)***
  The GDPR is vague as to the meaning of "data protection by design". The practical implications are therefore vague. This could in principle be onerous for organisations which may over-engineer (implying increased costs) or under-engineer (implying risk of data breach). An industry agreed design approach is required – this could be best addressed by an appropriate standard. ISO/IEC is working on the 27550 standard on "Privacy Engineering" which should cover this area.

- ***Security requirements***
  There is already an established certification system in place via ISO standards on security. Rather than creating a shadow certification system that only applies in the EU, consideration should be given to adopting relevant ISO standards that meet these criteria or seek updates to the standards that could be integrated at next re-certification stage by recipients of the standard. Given the already large compliance burden on many companies, the most efficient certification system should rely on existing compliant standards. For example, it is noteworthy that the standards subcommittee responsible for ISO/IEC 27001 is in the process of developing a new standard, ISO/IEC 27552, which is intended to extend ISO/IEC 27001 to include Data Protection. Such a standard is certifiable and could form the basis of a Data Protection certification scheme.

- ***Processor guarantees***
  The most appropriate approach is that a controller using one or more processors for

processing personal data collected by the controller, should be able to rely on (one or more) appropriate certifications held by the processors with respect to data protection. This is typically the practice for information security, where a customer requires a suitable security certification from any of the processors they use (e.g. cloud service providers).

- ***International transfers***

  - The relationship between GDPR certifications and other transfer mechanisms should be assessed. In particular, this assessment should include a review of the relationship with other data transfer mechanisms that work on the basis of a similar certification with which the EU schemes need to interact. This includes the EU/US Privacy Shield and the APEC CBPR.
  - Any new transfer-related certifications should, where possible, avoid creating conflicting requirements with other systems.
  - Certification should take into account existing transfer instruments. Clear guidance should also be provided on the relationship between certification and BCRs, EU-US Privacy Shield and APEC CBPR mechanisms.

Question 2: What other types of processing, services or products should be data protection certified, if any?

The GDPR does not specify the parameters for the object of certification. Article 42 merely refers to "processing operations" and Recital 100 to "relevant products and services". Therefore, the scope of certification should not be interpreted too narrowly and some flexibility should be provided to organisations. It could include, for example, a mobile application, an internet website, a privacy program or any specific product. The object of certification must be clearly articulated and distinguishable from non-certified products, processes, services or programs by and within an organisation. It is also important that consumer confusion is avoided.

Question 3: What would be an "appropriate level of expertise in relation to data protection" for a certifying body?

- At a minimum a certifying body would be expected to be staffed similarly to a data protection authority with lawyers, technical experts and auditors with proven data protection and technical expertise and competence.
- National accreditations bodies must accredit certifying bodies. Accreditation criteria for such bodies should be open to public comment and industry input.
- Certifying bodies should be set up to ensure the effective and practical participation of the private sector in the certification process. Taking into account that GDPR certification will cover different types of products, systems, processing as well as different type of enterprises

(micro, small, medium-sized and large-scale) the level of expertise should therefore not be strictly defined.

Question 4: What criteria should a supervisory authority approve to support data protection certification?

- Data Protection Authorities have wide powers under the GDPR. Inter alia, they have the power to issue, renew and revoke certifications, or where certifications are issued by "certification bodies", the DPAs approve the accreditation criteria for such bodies. They also play a key role in the accreditation of certification bodies.
- DPAs also have the power to disapprove or revoke individual certifications provided by certification bodies "where necessary." It should be further elaborated how this power will be implemented in a sensible way without introducing a new layer of review in each case. Appropriate criteria and a process must be developed for when and how to exercise this power, based on the idea that this power should only be exercised in exceptional cases.
- The accreditation of certification bodies would be a new task for DPAs and does not necessarily fit within their past experiences. It also bears the risk of regulatory conflict when the DPAs are required to take enforcement actions against companies, processes products or services certified by a certification body which the DPA itself has accredited. The risk of conflict of interest is even more pronounced when the DPA itself issues certifications which it must later enforce.
- Overlap and proliferation of certifications should be avoided to reduce consumer/stakeholder confusion or dis-incentivise organisations from seeking certification. Certification in support of the GDPR process should harmonise, consolidate and make interoperable existing mechanisms to take into account other systems and frameworks from within and without the EU. Any new transfer-related certifications should avoid creating conflicting requirements with other systems.
- The relationship between GDPR certifications and other data transfer mechanisms should be assessed. This assessment should in particular include the relationship with other data transfer mechanisms that work on the basis of a similar certification with which the EU schemes need to interact.
- There should be one EU baseline certification template for all contexts and sectors, which can be differentiated in its application by different certification bodies during the certification process.
- The differentiated application of this certification to specific sectors may be informed by sector-specific codes of conduct.

- Private sector organisations, including businesses that might seek certification and potential certification bodies, should have a meaningful role in the drafting and development of GDPR certification schemes and criteria.

Question 5: How can certification be made relevant for micro, small, medium-sized and large-scale enterprises?

In order for certification to be relevant for micro, small, medium-sized and large scale enterprises, a general and flexible EU-wide approach should be preferred. Such an approach would ensure clarity and avoid the confusion that the development of too many different certification mechanisms could produce. Certification should also be scalable and affordable to enable smaller enterprises to rely on this mechanism.

Question 6: Under what circumstances would it be appropriate for a certification to be withdrawn from an organisation?

- The withdrawal of a certification from an organisation would need to be context specific.
- If an organisation has shown itself not to meet the requirements specified in a certification, it should be required to re-certify to that standard. If it fails to do so then the certification should be withdrawn.
- Where an organisation can be shown to have demonstrated a wilful disregard for the requirements of the GDPR in relation to those areas for which it was certified, then removal of a certification could certainly be contemplated.
- Certification bodies also have a responsibility in this space. Trust in the certifications which they award are crucial to their overall acceptance among data subjects and data protection authorities.

Question 7: What information about a data protection certification award should an organisation make known to its users?

- This will be a matter for organisations in receipt of a certification.
- While certifications clearly have a potential to increase user trust, they must not be understood as an assurance to users that a recipient will be fully data protection compliant. This is especially the case where a certification might be awarded in one specific area but a data controller uses it to assure users across a broad spectrum. To reduce this risk, where certifications can be displayed there should be a requirement that they clearly outline the specific data protection compliance aspects to which they relate (e.g. security or transparency specific certifications).