DIGITALEUROPE

DIGITALEUROPE's input on Automated Individual Decision Making & Data Breach Notification (FabLab II Conference)

Brussels, 5 April 2017

EXECUTIVE SUMMARY

DIGITALEUROPE, as the voice of the digital technology industry in Europe, welcomes the opportunity to take part in the Article 29 Working Party's ("WP29") upcoming "FabLab II Conference", which will cover the topics of consent, data breach notification and profiling. DIGITALEUROPE continues to believe that the effective implementation of the General Data Protection Regulation ("GDPR") will require a joint effort between all stakeholders **built on mutual trust**. We therefore welcome the decision of the WP29 to host a second FabLab Conference aimed at gathering valuable in-person input from the data protection community.

As DIGITALEUROPE has been placed within the "consent" workshop and will be limited to providing in-person feedback to this sole issue, we wish to share with you our preliminary views on the topic of automated decision making, including profiling, and data breach notification which hold an equal level of importance for our members. DIGITALEUROPE has structured our comments in the following manner.

Automated Decision Making, including Profiling:

- Scope of Article 22
- The right not to be subject to a decision
- A decision based solely on automated processing
- The right to obtain human intervention on the part of the data controller, to express his or her point of view and to contest the decision
- Additional rights to information
- Profiling related to direct marketing
- Profiling and data protection impact assessments

Data Breach Notification:

- Practical implications for organisations
- Interpretation of 'risk to the rights and freedoms of natural persons'
- Interpretation of 'high risk to the rights and freedoms of natural persons'
- Circumstances in which a data controller should be considered to have 'become aware' of a data breach
- Circumstances in which it is not feasible to report a data breach within 72 hours
- Interpretation of provisioning notification information 'in phases without further delay'

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

- Interpretation of measures considered sufficient to mitigate adverse effects arising from a data breach
- Interpretation of measures considered sufficient to ensure that a high risk to the rights and freedoms of the individuals affected will not materialise
- Interpretation of 'disproportionate effort' in notifying individuals
- Interpretation of what form of public communication to inform individuals would constitute an equally effective manner when notifying the individuals concerned would involve a disproportionate effort
- For how long should a data controller be required to retain documentation relating to data breaches
- What level of detail needs to be provided when notifying a data breach

OVERALL VIEWS

The provisions on automated individual decision making, including profiling, and data breach notification were some of the most intensely discussed topics during the legislative discussions on the GDPR. The insurance, banking, telecommunications, healthcare, transport, and retail industries will all face different challenges on how these provisions apply to their sectors.

DIGITALEUROPE **fully understands the increased risks faced by data subjects** by the potential misuse of profiling. We believe that the drafting of Article 22 and other related provisions within the GDPR have **successfully found the fine balance** between stricter rules on the types of profiling that carry high risk for individuals and workable rules for all other types of profiling that do not negatively impact data subjects and are the cornerstone of Europe's data economy.

DIGITALEUROPE also notes that the text of the GDPR presents several critical areas where further clarification would be welcomed on the issue of data breach notification. The precise timing and means to notify a personal data breach **should not be used as a means to punish organisations or dis-incentivise responsible investigation and incident response**. Data protection authorities ("DPAs") should instead 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. If a proper balance is struck, we strongly believes that the data breach provisions of the GDPR should incentivise organisations to invest in a high degree of data protection.

We wish to outline below our reading of the letter of the law and suggest areas where further guidance would be useful in order to help companies understand how to plan their compliance programmes.

SPECIFIC CONCERNS – AUTOMATED INDIVIDUAL DECISION MAKING

1. Scope of Article 22

As clarified in Recital 72, DIGITALEUROPE considers automated individual decision making, including profiling, as a type of data processing that is subject to the general rules of the GDPR governing the processing of personal data. However, certain forms of automated decision making, including profiling are subject to the specific rules laid down in Article 22. DIGITALEUROPE would welcome recognition from the WP29 in its future draft guidance document that Article 22 applies to automated decision making, including profiling, when the following cumulative conditions exist:

- A *decision* – An 'action' on part of the data controller or data processor, which relates to a specific individual. This should exclude all types of analytics that take place in order to, for example, improve a service without a decision taken in relation to a specific individual;
- Based *solely* on automated processing – Where there is human contribution to the making of such a decision, the data processing falls under the general rules of the GDPR; and
- Which produces *legal effects* concerning him or her – We would appreciate clarification in the future guidance on what can be considered to constitute 'legal effects' as well as examples of such effects in different sectors;

  OR

- Which *similarly significantly affects* him or her – We believe the effects should be 'similar' to a legal effect AND 'significant'. We would appreciated clarification in the future guidance on how companies should interpret these two cumulative conditions as well as examples of such effects in different sectors.

2. The right not to be subject to a decision

DIGITALEUROPE understands the right not to be subject to a decision of Article 22 as the information right on the existence of profiling with the option to opt-out. We also note that from the point of view of a company that is currently designing specific mechanisms to be able to satisfactorily respond to the exercise of the various rights of data subjects set out in the GDPR, we would welcome clarity whether this right is different in practice from:

- The right to object as found in Article 21 – We assume this is a right that can be exercised in response to a decision (i.e. it allows a data subject to contest the decision); and
- The obligation for data controllers to ensure that it is possible for data subjects to exercise the right to withdraw consent at any moment as foreseen in Article 7(3).

3. A decision based *solely* on automated processing

Based on the inclusion of the term 'solely', DIGITALEUROPE understands that if there is human involvement or oversight of the *decision* made, such a decision would fall outside the scope of the article. For instance, this would be the case when the selection of rules and data included in an analytical model are determined by a human, or are tested by a human before being deployed in production or are periodically reviewed by a human.

DIGITALEUROPE would welcome clarification in the draft guidance on what type of decisions based *solely* on automated processing would be considered to be covered by this article.

4. The right to obtain human intervention on the part of the data controller, to express his or her point of view and to contest the decision

Automated individual decision making, including profiling, that falls within the scope of Article 22(1), can still take place inter alia under the conditions set out in Article 22(2)(a) and Article 22(2)(c), as long as the data controller implements suitable measures to safeguard the rights, freedoms and legitimate interests of the data subject. We note that these 'suitable measures' should include the right to:

- Obtain human intervention on the part of the data controller – The scale at which data controllers operate and the speed at which it is necessary to make decisions in relation to security and indeed fraud for instance, the possibility for human intervention in such circumstances will arise after a decision;
- Express his or her point of view – We would welcome from the WP29 examples of how companies can plan to provide this right in practice in different sectors;
- Contest the decision – We would welcome from the WP29 examples of the mechanism that should be foreseen by companies in different sectors in order to satisfy this right; and
- Obtain an explanation of the decision reached after such assessment – Recital 71 adds this example as a 'suitable measure' and we would welcome from the WP29 clarity on what 'such assessment' refers to.

5. Additional rights to information

As set out in Recitals 60 and 63, in addition to the information requirements foreseen in the general rules of the GDPR governing the processing of personal data, data subjects have the right to obtain the following information:

- When profiling takes place – The *existence* and *consequences* of the profiling;
- When automated decision making, including profiling, takes place – The *logic involved* in any automated personal data processing; and
- When specific types of automated decision making, including profiling, that fall within Article 22(1) and Article 22(4) takes place – The *existence*, the *logic involved*, the *significance*, and the *envisaged consequences* of such processing.

DIGITALEUROPE interprets these provisions in accordance with Article 12, which specifically references Article 22 and notes that the information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. We wish to note that information regarding the existence, consequences and logic of profiling can be extremely complex given the technology processes often involved. We believe that it may be useful for the WP29 (together with stakeholders) to develop standard language for specific types of profiling that the consumer will easily recognise and understand. Furthermore, according to the requirements laid down in relevant laws, organisations should not be expected to reveal information that pertains to protected trade secrets and intellectual property. Equally, the information required to be provided should not be capable of allowing a bad actor to game systems and thereby compromise security and perpetrate fraud.

6. Profiling related to direct marketing

DIGITALEUROPE recognises that when profiling is related to direct marketing, data subjects have the right to:

- Object to initial or further processing at any time free of charge; and
- Be informed explicitly about their right to object and presented this information clearly and separately from any other information.

In light of the above, DIGITALEUROPE believes it would be helpful to receive clarity on how the 'right to object' in this respect is different from the 'right not to be subject of' as laid down in Article 22. Moreover, clarity would also be welcome on how the provisions of the ePrivacy Directive regarding e-marketing, which can include direct marketing, apply *lex specialis* in relation to the GDPR.

7. Profiling and data protection impact assessments ("DPIAs")

When considering the interplay between profiling and DPIAs, DIGITALEUROPE understands that DPIAs in accordance with Article 35(3)(a) are only required for:

- A systematic and extensive evaluation of personal aspects to natural persons; and
- Automated processing, including profiling, that falls within the scope of Article 22 as previously described.

We would welcome clarity in the WP29 guidelines affirming this interpretation.

SPECIFIC CONCERNS – DATA BREACH NOTIFICATION

1. Practical implications for organisations

The GDPR sets out several steps in responding to a potential or suspected 'incident', which may ultimately be determined to be a 'personal data breach'. The requirement that an organisation report to a DPA the 'consequences of the personal data breach,' as set forth in Article 33(3)(c), will present a particular challenge for organisation as anticipating potential outcomes is an exercise in prognostication balanced by risk management. This requirement should be interpreted to require data controllers to provide recommendations to the DPA as to how to reduce or mitigate potential impacts and harms resulting from a personal data breach.

We believe that the notification to data subjects presents a vital opportunity for those impacted by a data breach to take action to protect their rights and freedoms. DIGITALEUROPE encourages the creation of a reasonable standard that permits for the appropriate investigation and consideration that 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.

Furthermore, we believe that there is a need for DPAs to provide further guidance on 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. Where co-operation is required in an investigation between DPAs this should take place within the context of the co-operation arrangements specified in the GDPR.

2. Interpretation of 'risk to the rights and freedoms of natural persons'

While Recital 85 sets forth certain examples of what 'risks to the rights and freedoms of natural persons' could entail, we encourage DPAs to be 'less prescriptive' about such risks. As organisations are charged with evaluating risks in light of a data breach, certain risks - such as discrimination - may be inordinately challenging to pre-define. Instead, we **encourage further discussion and the development of informal and interpretive guidance** as DPAs and data controllers alike manage reporting requirements under the GDPR.

3. Interpretation of 'high risk to the rights and freedoms of natural persons'

Recital 86 sets forth circumstances where 'high risk' may exist, including the existence of 'immediate risk of damage' or the need for individuals 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.

4. Circumstances in which a data controller should be considered to have 'become aware' of a data breach

DIGITALEUROPE stresses that 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. We believe the future guidance should reflect the fact that data controllers must not be considered 'aware' of a data breach merely because such an incident is suspected. Furthermore, **the 72-hour requirement should not commence merely due to public reporting of a potential incident impacting the data controller, including by third parties**. DIGITALEUROPE wishes to draw the WP29's attention to the many instances of media reports of claimed data beaches, which have transpired to have no substance. The prospect of a reporting requirement cannot become a means by which criminals can pressurise data controllers to pay ransoms, etc. to avoid a matter becoming the subject of media reports.

As such, in the future guidance, we believe that data controllers should be considered as 'aware' of a data breach upon:

- **Actual knowledge or confirmation of such a breach by responsible officers within a data controller** - A report by a concerned customer, without supporting evidence, should 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; and
- **Conclusion of investigation** - Where a personal data breach is suspected, at the conclusion of a reasonable and appropriate investigation under the circumstances and the suspicion is confirmed.

5. Circumstances in which it is not feasible to report a data breach within 72 hours

DIGITALEUROPE notes that there are innumerable circumstances in which it would not be feasible for a data controller to report within 72 hours of becoming aware of a data breach. Given the often multinational nature of data security incidents, there can be complex and conflicting mandatory reporting and non-disclosure obligations. The needs or requests of law enforcement in various jurisdictions can also complicate such efforts. Furthermore, 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. The 72 hour deadline could also be particularly challenging in certain complex outsourcing deals where there are various parties involved.

6. Interpretation of provisioning notification information 'in phases without further delay'

DIGITALEUROPE emphasises that it is vital that data controllers providing initial or interim notifications of a data breach to a DPA are **afforded appropriate flexibility to report only that information relating to the breach which is confirmed or believed to be true**. It should be expected that a data controller that does not have all of the information required to provide a notification at the time of initial contact, and that as such the data controller is conducting an active investigation. As the future guidance 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 maximum extent, it is vital that DPAs **not initiate investigations or pose unnecessary questions during this 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 DPA should be expected to launch an immediate investigation.

7. Interpretation of measures considered sufficient to mitigate adverse effects arising from a data breach

DIGITALEUROPE believes that 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 and potentially provisioning of some form of 'identity theft monitoring.' However, the future guidance should not note that these services should be required in response to all data breaches. Instead they should be selectively employed where necessary and appropriate. **There is no one-size-fits-all measure**, although measures that are aligned with international standards should be encouraged.

Moreover, Article 33(3)(c) should be interpreted to as an avenue for data controllers to provide information on how data subjects may mitigate adverse events as each data subject will have an individualised assessment of what potential adverse effects may accrue from a data breach. Finally, the future guidance should note that data controller can mitigate adverse events, including as related to an ongoing potential breach, by remediating underlying issues.

8. Interpretation of measures considered sufficient to ensure that a high risk to the rights and freedoms of the individuals affected will not materialise

DIGITALEUROPE stresses that 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 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**. For example, a set of data subjects may provide health information and records to a data controller with the expectation that such records are made available to any researcher or student that is interested. However a well-intentioned individual who is not a researcher or student may accesses such data, which is later discovered by the data controller. While such data is undoubtedly sensitive the mere fact that such information is accessed would not necessarily lead to the classification of the breach as one that poses a high risk to individuals. The guidance should encourage data controllers 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 without consideration of all the facts.

9. Interpretation of 'disproportionate effort' in notifying individuals

DIGITALEUROPE notes that 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, the future guidance should emphasise that **data controllers should not in all cases be required to affirmatively prove contact with each individual**, and it should be considered a 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.

10. Interpretation of what form of public communication to inform individuals would constitute an equally effective manner when notifying the individuals concerned would involve a disproportionate effort

DIGITALEUROPE stresses that given the increasingly interconnected nature of the world, effective public communication can take a number of forms. While certain forms of communication can be pre-judged to be effective, such determinations should not be prescriptive and grounded in the draft guidance. Certain existing and broadly-available forms of communication (e.g. posting a notice to a data controller's webpage, issuing a press release to major services, a Twitter message, etc.) 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, especially when taking into consideration consequent media attention, may be more than sufficient to put data subjects on notice.

11. For how long should a data controller be required to retain documentation relating to data breaches

DIGITALEUROPE believes that absent an independent legal responsibility to retain documentation, such as ongoing legal proceedings, **data controllers should retain documentation in accordance with existing internal policies**. DIGITALEUROPE cautions against the draft guidance including distinct retention requirements as this potentially increases risk to data subjects (should their personal data be included in such documentation) and complexity that may disrupt existing, potentially mature organisational processes.

12. What level of detail needs to be provided when notifying a data breach

DIGITALEUROPE notes that Article 33(3) of the GDPR provides some direction as to the details of the information that should be provided by organisations when notifying a data breach. We encourage the future draft guidance to reflect that the **security of organisations must be respected** and that a breach notification should not provide extensive details on the technical and organisational measures implemented by the organisation. We take note of Article 33(3)(d), but would welcome clarification that **not all the technical details surrounding the mitigation measures be disclosed a**s this may impact confidentiality and intellectual properly concerns.

CONCLUSION

DIGITALEUROPE once again wishes to thank the WP29 for providing the European digital technology industry with the opportunity to take part in the upcoming "FabLab II Conference". It is of paramount importance that data controllers and data processors receive legal certainty and clearly understand how the provisions related to automated decision making, including profiling, and data breach notification should be implemented and enforced. We trust that the WP29 will work to include the feedback it receives from stakeholders prior to, during, and following the FabLab II into its final guidance documents. We look forward to providing more detailed feedback once the draft guidance has been published and would like to extend the offer to meet with the WP29 if you have any specific questions or require further input given the technical nature of the issues involved.

--

For more information please contact:
Damir Filipovic, DIGITALEUROPE's Director (Digital Consumer and Enterprise Policy)
+32 2 609 53 25 or damir.filipovic@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies.

DIGITALEUROPE ensures industry participation in the development and implementation of EU policies. DIGITALEUROPE's members include 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Airbus, Amazon Web Services, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, iQor, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric IT Corporation, Sharp Electronics, Siemens, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: ICT IRELAND
Italy: ANITEC
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK