AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Working Party 29 draft Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive summary

We welcome the fact that WP29 is aiming to adopt guidelines on Automated individual decision-making and Profiling. These types of processing are covered by complex provisions in the GDPR and raise challenges in various sectors.

Many issues are being addressed in the draft guidelines with helpful recommendations. We focus here on points that we believe require further attention in view of the finalization and adoption of the guidelines.

Contents

How the GDPR applies to automated decision-making and profiling

We welcome the guidelines, recognize the specific scope of Article 22 and address separately automated decision-making including profiling that falls within the scope of the general provisions of the GDPR. We also note that there should be resistance to gold-plating what is already a strong provision within the Regulation.

We believe however that section 'C. How the GDPR addresses the concepts' (page 8) should be reviewed to properly reflect the structure of the GDPR, which we understand to be the following:

1. When personal data is processed in the context of profiling or automated decision-making, the general GDPR provisions apply (reiterated in Recital 72).
2. When automated decision-making, including profiling, takes place, the GDPR foresees specific requirements as set out in the guidelines. We note here that from a strictly legal point of view, the GDPR restricts most related provisions to profiling that includes a 'decision that has a legal or similarly significant effects'. Therefore, we suggest that, for the purposes of clarity, the guidelines expressly note that the general GDPR frameworks applies to 'general profiling', while specific requirements apply to decision-based categories of profiling.
3. Article 22 applies to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Definition of profiling

We welcome that WP29 guidelines rightly begin by acknowledging the positive impact of profiling and automated decision-making by stating that it can be useful for individuals, organisations, the economy and society as a whole. It is useful that the guidelines specify that when it comes to commercial applications, it can be used to better segment markets and tailor services and product to align with individuals' needs. In most cases, profiling is about serving people, and it is for that purpose that most organisations rely on profiling and automated-decision making. It is important that individuals can have a clear understanding that profiling and automated decision-making can be to their benefit.

The guidelines should include additional developments on the positive value of profiling and on the benefits that it can bring to individuals, organisations, the economy and society as a whole. This should not be limited to the introduction of the guidelines. Positive examples of profiling and automated decision-making should be provided in all sections. To this end, we provide some examples at the end of this paper (page 13).

Scope of Article 22 - "decision"

Section 'II. Specific provisions on automated decision-making as defined in Article 2' of the guidelines (p. 9) analyses the wording of Article 22§1 to help define its scope. It is an important omission to not include any analysis of the word 'decision'. During the legislative process there were extensive discussions on the term (including discussions on whether the wider term 'measures' should be used

instead). A 'decision' requires an 'action' from the data controller or data processor, which relates to a 'specific' individual as indicated above. This excludes from the scope of Article 22 (and not the GDPR general provisions of course) all types of analytics that take place in order to, for example, improve a service without a decision being taken in relation to a specific individual.

Based on this analysis, the following statement on page 6 of the guidelines is not accurate: 'The GDPR does not just focus on the decisions made as a result of automated processing or profiling. It applies to the collection of data for the creation of profiles, as well as the application of those profiles to individuals'. The GDPR does focus on the final 'decisions' both in Article 22 and all other provisions that relate to automated decision-making as indicated above because the 'decision' is the part of the technical process that carries the greater risk for the individual. All other parts of the technical process starting with the collection of data for the creation of profiles remain regulated under the general provisions of the GDPR.

Similarly significant effect

We welcome the effort to clarify the threshold of Article 22 in relation to the wording 'similarly significantly affects him or her'. This is definitely a point that creates legal uncertainty in practice. The guidelines (page 10) however focus more on the interpretation of the word 'significant' i.e. the 'degree' of the impact on the individual and not on the word 'similarly', i.e. the 'type' of impact on the individual which is required to have similar significance to a legal effect. The latter wording in the threshold is indeed what is harder to interpret in practice given that, as the guidelines state, the word 'similarly' was not present in Article 15 of Directive 95/46/EC and is introduced by the GDPR.

The WP29 guidelines helpfully recognise that to be within the scope of Article 22, decisions having 'similarly significant effect' must have effects that are more than trivial and must be significantly great or important to be worthy of attention. The WP29 should make clear that as a rule, targeted advertising does not have 'similarly significant' effects and that Article 22(1) should only cover situations where the decision would have significant effects on an individual, which cannot be the case of targeted advertisement. In fact, as far as advertisement is concerned, individuals are merely presented information that does not affect the ability to purchase any other service or product nor does the advertisement deny any right to the individual. Marketing activities more generally aim at presenting consumers with products they may enjoy. A typical example is to suggest to consumers who use a middle-tier brand to discover either a premium brand or the latest category innovation introduced in the market. Most of these activities involve non-sensitive personal information and present a very low level of privacy intrusion. As such, notwithstanding consumers' right to object as defined by Article 21(1), we believe guidelines should specify that this type of activities should not fall under Article 22(1).

The WP29 then provides a confusing example to illustrate how targeted advertisement could have 'similarly significant' effects: the case of an individual in financial difficulties who is regularly shown adverts for on-line gambling, who may sign up for these offers and potentially incur further debt. The example is misleading. It should be made clear that this would only cover situations where the controller has actual knowledge of the particular situation of the individual and that despite this knowledge it would wilfully target (wilful manipulation) that specific advert to the individual. Furthermore, the controller should not be compelled to collect extra information just for the sake of

acquiring such actual knowledge, as that would be overly privacy invasive, inconsistent with the minimisation and proportionality principles, and in some cases going against the spirit as well as the letter of article 11(1) on processing not requiring identification.

Moreover, the WP29 does not give any definition of the four characteristics listed in the guidance. It should be specified that those criteria are cumulative and the criteria of 'actual knowledge' and 'wilful manipulation' should be added.

Furthermore, the guidelines do not provide sufficient guidance also as regards the 'significance', i.e. the degree of impact. The phrase 'effects of the processing must be more than trivial and must be sufficiently great or important to be worthy of attention' (page 10) is too vague to be meaningful in organisations' compliance efforts. Also the following sentence is not helpful: 'the decision must have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned'. We need more guidance around the term 'significantly' and this term's use in the explanation.

On page 10, the guidelines also quote examples from recital 71 as examples of automated decisions with a 'similarly significant' effect, and not a legal effect. However, they clearly have legal effect and citing them as examples of 'similarly significant' (i.e. non-legal) effects would lead to confusion.

Finally, a few more points in this section of the guidelines do not offer a pragmatic interpretation or helpful guidance:

- We are also concerned by the following statement on page 11: 'Automated decision-making that results in differential pricing could also have a significant effect if, for example, prohibitively high prices effectively bar someone from certain goods or services'. It is too generic and seems to imply that differential pricing may always fall in the scope of this article. We note that of course when differential pricing is based on illegitimate factors and is discriminatory, it is prohibited anyway under different rules.

- 'Positive' similarly significant effects should not be included in the threshold and only results in creating confusion. Where automated decisions have a positive effect (e.g. health and social benefits), they should not be considered to have a 'similarly significant effect' and should therefore not be considered as a 'prohibited' automated decision under Article 22 of the GDPR. This has the advantage of ensuring that individuals get the (e.g. health and social) benefits from such automated decisions even if they have forgotten to submit a certain consent form. At a minimum, automated decisions with a merely positive effect should be subject to a less strict regime in terms of transparency requirements for automated decisions, in particular, in relation to the requirement to provide meaningful information about the logic involved, the significance and the envisaged consequences of the automated decisions.

  Furthermore, the current interpretation provided in the guidelines would not be in line with the risk-based approach of the GDPR also because it was clear during the legislative process that the intention of the legislators was to protect the individual from negative and harmful effects (alternative wording considered throughout the legislative process included 'discriminatory' or 'adverse' effects).

- The guidelines refer to the notion of 'substantially affects' defined in the Lead Authority WP29 Guidance as a helpful concept to interpret similar significant effects. The notion of substantially affects is particularly broad and includes for example 'well-being or peace of mind' of the individual. Such a broad interpretation is against the spirit of 'similar significant effect' to a legal effect. This reference should be deleted.

- Possible effects that 'may also be triggered by the actions of individuals other than the one to which the automated decision relates' according to the guidelines are practically impossible to assess and puts a disproportionate burden on the controllers. How do we define who those other individuals may be, how do we estimate the possible actions of each of those individuals and how do we assess the possible effects of those possible actions on the individual being profiled? This cannot serve as a criterion to determine whether a practice meets the threshold in question and should be deleted.

The 'prohibition' of Article 22(1)

The WP29 interprets Article 22(10 as a blanket prohibition against automated decision making having a legal effect or similar significant effects. It is not in line with the wording of recital 71 and Article 22 (1) of the GDPR. Article 22(1) should be interpreted as establishing a right for the data subjects. This is a right that requires a positive action by the data subject, who must inform the data controller (upon receiving the required transparency information on the automated decision) that he/she does not wish to be subject to the automated decision. The interpretation of the structure of this article is based on the letter of the law and recognizes that the article establishes a right to be invoked by the data subject and not a prohibition. This is aligned with other GDPR rights which also require a positive action (e.g. notice requirements (Art. 13(2)(f), Art. 14(2)(g) and right to access Art. 15(2)(h)), with the purpose of alerting the individual of the right in Art. 22. Consequently, paragraph 2 does not include 'exceptions' but rather sets out cases when paragraph 1 does not apply. This interpretation is not only in line with the letter of the law but also the intention of the legislature; many legislative amendments considered throughout the legislative procedure would have established a clear prohibition (notably tied with wording related to "adverse" or "discriminatory" effects as described above), but these were rejected and the legislature adopted a different approach.

This interpretation is further supported by the implementation by several data protection authorities of the current Article 15 of EU Directive 95/46/EC, which has substantially similar language to that of Article 22 (1) of the GDPR. For example, Article 12(1) of the UK Data Protection Act, which implements Article 15 of the EU Directive 95/46/EC, provides that each data subject 'is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data'. We note that there are other protective measures under the GDPR such as notice requirements (Art. 13(2)(f), Art. 14(2)(g) and right to access Art. 15(2)(h)), with the purpose of alerting the individual of the right in Art. 22.

As a consequence of an interpretation of Article 22(1) as a positive right not to be subject to ADM having legal effects or similar significant effects, data subjects would be entitled to an unconditional right to object before or after the decision is taken. Implementing it as a right to be invoked is more in line with modern data processing realities.

The right to be informed

We believe that the GDPR does not require an approach that would result to "ensuring that information about the profiling is not only easily accessible for a data subject *but that it is brought to their attention*" as specified in the guidelines (page 13). As explained in the guidelines, in relation to profiling the GDPR requires in Recital 60 that 'the data subject should be informed of the existence of profiling and the consequences of such profiling'.

Organisations may also choose to go beyond the legal requirements in this respect to obtain a competitive advantage. But the GDPR does not require organisations to inform data subjects in this respect in a manner that is different from other instances in the sense implied by the guidelines. We are also concerned that such an interpretation by WP29 may lead to excessive notices to data subjects. It is generally acknowledged that 'notice fatigue' can have an adverse effect on meaningful privacy protection.

Furthermore, it would be helpful to make a clearer distinction in the guidelines as regards the different information provision obligations that relate to automated decision-making and profiling. In addition to the information requirements foreseen in the general rules of the GDPR governing the processing of personal data including Article 12, we would recommend an overview including Recitals 60 and 63, which shows more clearly that data subjects have the right to obtain the following information:

- When **profiling** takes place – The **existence** and **consequences** of the profiling (Recital 60);
- When specific types of automated decision making, including profiling, that fall within **Article 22(1) and Article 22(4)** take place – The **existence**, the **logic** involved, the **significance**, and the **envisaged consequences** of such processing.

Regarding the logic involved behind automated decision-making, we welcome the fact that the working party insists on the need to find simple ways to tell individuals about the logic behind the decision and the algorithm used. Although the information should of course be meaningful, it should not be a complex explanation or a disclosure of the algorithm. There should be specific clarification in the guidance that there is no requirement to disclose algorithms or intellectual property, in whole or part, to a data subject. Full transparency of algorithms, namely disclosure of source code, raises important legal problems from intellectual property and trade secrecy perspectives, just like the disclosure of other types of proprietary information (eg. software, patents) as recognised in Recital 63. Any disclosure requirement must only be in specific cases where there is a requirement by authorities, e.g., in the case of a law enforcement or fraud investigation, and not to individual data subjects. Finally, full transparency is not meaningful to users and does not advance the understanding of how their data is being handled. In fact, disclosure of source code or extensive description of the inner logic of algorithms, which is only understandable by experts, will not contribute to explaining to users how automated decision processes are attained; on the contrary, it may do the opposite, overwhelming and confusing them even more.

In several parts, the guidelines go further than GDPR requirements:

In particular, the GDPR does not require an approach that would result in 'ensuring that information about the profiling is not only easily accessible for a data subject but that it is brought to their

attention' as specified in the guidelines on page 13 Therefore we urge the WP29 to clarify that providing this information in a privacy policy would be sufficient.

Similarly, on page 20 where the guidelines read 'In all cases, data subjects should have enough relevant information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice', the 'envisaged use' goes much further than the 'existence' required by the GDPR in relation to profiling.

Finally, we also note the example on page 23 where the guidelines read 'The data subject should also be given information about their profile, for example in which **segments** or **categories** they are placed'. Given that at this point in the example the processing does not fall under Article 22, the GDPR would not require the level of detail that extends to 'segments' or 'categories' in the general information provision obligation of the controller which relates to the fact that profiling is taking place. This information may indeed be required by the GDPR if the data subject exercises their right to access the profile.

Data Protection Principles

The interpretation provided of Article 5(1) (e) on Storage limitation in page 20 is not helpful in relation to profiling and automated decision-making. Firstly, the general principle of Article 5.1(e) of GDPR provides for personal data to be retained for as long as 'necessary for the purposes for which the personal data are processed'. This should not be different for profiling and the data controller should be able to process the data for the purpose of automated decision-making and for as long as is necessary. WP29 should specify that such data should be regularly reviewed as in accordance with the section above on accuracy.

In addition, retaining personal data for longer periods may actually increase the accuracy of the profiling undertaken with such data. The technology behind profiling is such that the more data are taken into account by the profiling algorithm, the more accurate the profiling will be. Storing the data for longer periods will therefore be advantageous for data subjects, as it ensures that any profiling relating to such data subjects is as accurate as possible.

Secondly, the words 'lengthy periods' and 'too long' are vague terms. It is unclear who will determine what a 'lengthy period' and 'too long' means. This could have the consequence that, even if data is still necessary for automated decisions, a data controller could deem that it has retained the data "too long" and therefore delete it. Such a decision would have two consequences: (i) the profiling would become less accurate (as explained above), and (ii) data subjects would suddenly be confronted with their data (e.g. their photos, website orders, transaction history) no longer being recoverable**. We therefore suggest deleting the vague terms 'lengthy periods' and 'too long' and simply referring to the above-mentioned principle of Article 5.1(e) of the GDPR.**

Article 6 – Lawfulness of processing

The WP29 adopts a very narrow interpretation of consent by asserting that where consent to profiling is a pre-condition of accessing the controller's services, 'consent is not an appropriate basis for the

processing'. This could exclude the possibility for many companies offering free services online to rely on consent. People know that many services— from online publications to music streaming services to social networks— are able to operate without charging people who use the service because they show ads, and that ads are based on the interests that individuals express online. Individuals should be able to decide by themselves. **T**he WP29 should confirm that consent is an appropriate legal basis for profiling and that withdrawal of consent can be served by not providing a service anymore. Consent should be considered as an appropriate basis when it is supported by control mechanisms like the possibility to edit preferences categories according to which advertisements are delivered.

The Working Party provides an example of processing that would not be necessary for the performance of a contract: 'a user buys some items from an on-line retailer. In order to fulfil the contract, the retailer must process the user's credit card information for payment purposes and the user's address to deliver the goods. Completion of the contract is not dependent upon building a profile of the user's tastes and lifestyle choices based on his or her visits to the website'. This example gives a very narrow interpretation of the 'contractual necessity' legal basis and affects the ability that organizations have to define their own services. Online services are based on the concept of personalisation. The ability to provide a service fully tailored to the needs of their users is at the core of what many internet companies do. It can in fact be an inextricable aspect of the service they provide and be one of the main objects of the contract itself.

The WP29 guidelines provide some elements to take into account for the balancing test that must be carried out when a data controller relies on legitimate interest: the level of detail of the profile, the comprehensiveness of the profile, the impact of the profiling (the effects on the data subject), and the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process. These elements are not detailed enough to understand how they should be used in the balancing test:

- The level of detail of the profile and comprehensiveness of the profile: the balancing test should focus on the uses of the profile rather than on the information collected to build the profile.
- The impact of the profiling: the impact of the profiling can be positive on the data subject. The WP29 should clarify that in that case the interests of the data subject are appropriately safeguarded. In general, it should be considered that the use of a profile should not have significant adverse impact on the data subject.
- Safeguards to ensure fairness, non-discrimination and accuracy: It should be clarified that the legal concept of direct discrimination is used, i.e. the disadvantageous treatment of an individual based on a ground prohibited by law.

Article 9 - Special categories of data

We recognize that specific attention is required for special categories of data but the guidelines go beyond the GDPR requirements as regards the information provision obligation. On page 22, the guidelines suggest that 'The controller should make the data subject aware that not only do they process (non-special category) personal data collected from the data subject or other sources but also that they derive from such data other (and special) categories of personal data relating to them'.

The GDPR obligation to provide information relates to the processing of personal data. The outcome of the processing should not be subject to an additional obligation to inform data subjects. If new processing of personal data takes place on the basis of this outcome, the rules on further processing would apply. Obviously also from a practical point of view, it is often impossible for the controller to inform on what may be 'derived' before the processing takes place. And from the point of view of the data subjects, this would result in providing complex information that would not necessarily help their understanding of the processing in the frame of informed consent.

Article 5(1) (d) - Accuracy

The principle of accuracy is very stretched on page 19 of the guidelines that refer to 'a dataset that may not be fully representative or analytics that may contain hidden bias beyond the accuracy of raw data'. In addition to GDPR Article 5(1) (d) which requires the accuracy of personal data, in relation to automated decision-making and profiling, we note the GDPR requirements in Recital 71 '[…] the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized […]'. We therefore suggest that both from a legal and technical perspective the guidelines do not offer a helpful interpretation by extending the principle of accuracy to 'analysing data', 'building a profile for an individual' and 'applying a profile to make a decision affecting the individual'.

Article 15 – Right of access

It seems unnecessarily restrictive to provide that it is only under "rare circumstances" that the controller's trade secrets and IP rights should outweigh individuals' right of access. The right to protection of business secrets is a fundamental principle of EU law and the right to property is protected under Article 17 of the Charter, which provides no indication that certain of the fundamental rights enshrined therein necessarily trump the other rights.

Article 16 - Right to rectification

The guidelines read as follows on page 24 'The right to rectification applies to the 'input personal data' (the personal data used to create the profile) and to the 'output data' (the profile itself or 'score' assigned to the person, which is personal data relating to the person concerned)'. This approach is not in line with the GDPR and raises concerns. The right to rectification applies to 'input personal data'. But data subjects cannot request to rectify the 'output data' (we note that the guidelines refer to 'output data' and not to 'output **personal** data' as opposed to 'input personal data') which can be based on complex algorithms that may include trade secrets or intellectual property. Would it be realistic that every credit score would need to be rectified on the data subject's request based on data protection grounds? Similarly, would this process make sense for energy companies that use smart meter data to, for instance, forecast energy demands? The right to rectification of 'output' data should

be restricted to Article 22, i.e. when the output is a decision having legal effect or similar significant effect.

The rectification of 'input personal data' may involve automatically the rectification of output data to some extent, but the scope of the right to rectification does not extend to 'output data' –as opposed to the right of access which also applies to 'output data'. To reinforce this analysis, it is useful to look at the right to data portability, in relation to which WP 29 guidelines clarify that inferred or derived data (i.e., the profile itself or the score in the example above) are not included in the scope of the obligation. The relevant WP 29 guidelines read on page 8 'In contrast, inferred data and derived data are created by the data controller on the basis of the data 'provided by the data subject'. These personal data do not fall within the scope of the right to data portability. For example, a credit score or the outcome of an assessment regarding the health of a user is a typical example of inferred data. Even though such data may be part of a profile kept by a data controller and are inferred or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as 'provided by the data subject' and thus will not be within scope of this new right.

Article 17 – Right to erasure

The guidelines suggest on page 25 that 'similarly the right to erasure (Article 17) will apply to both the input and the output data'. Following the same thinking as outlined above in relation to the right to rectification, the 'output data', i.e. the profile itself should not automatically be subject to the right to erasure. To the extent that the profile relates to an identified or identifiable individual, it should be erased when the right is exercised to the extent that this is required. In any case often such profiles are used in organisations in ways that no longer identify the individual, in which case the right to erasure would not apply. Therefore, the profile itself would need to be erased only in the cases where it qualifies as personal data under the GDPR.

Data Protection Impact Assessments

The guidelines read on page 27: 'Article 35(3) (a) refers to evaluations including profiling and decisions that are 'based' on automated processing, rather than 'solely' automated processing. We take this to mean that Article 35(3) (a) will apply in the case of decision-making including profiling with legal or similarly significant effects that is not wholly automated, as well as solely automated decision-making defined in Article 22(1).'

We agree that the provision includes decision-making that is not wholly automated, but we would like to clarify that Article 35(3) (a) only covers automated decision-making including profiling that otherwise falls within the scope of Article 22. This is clear in Article 35(3) (a) of the GDPR which reads '[…] which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'.

Children and Profiling

The WP29 guidance states: 'Because children represent a more vulnerable group of society, organizations should, in general, refrain from profiling them for marketing purposes.'

The WP29 statement references a study on marketing to children aged 6 to 12 yet, as written, it could be interpreted more broadly, to apply that study's findings to anyone under 18. That implies that anyone under 18 should not be exposed to personalized advertising, irrespective of whether consent has been obtained. The WP29 should clarify what 'children' means.

Such an approach would be inconsistent with the GDPR's existing protections for children, where children of 16 years (or from 13-16, depending on member states' discretion) are deemed mature enough to give consent to the processing of their personal data without parental authorization.

As written, WP29's draft guidance may be interpreted to mean that a 16-year-old cannot lawfully consent to personalized advertising (given that consent is likely to be the lawful basis for much personalized advertising under the GDPR). This position is out of step, given that a 16-year-old in many member states can lawfully consent to sex, marriage or surgical treatment, or join the armed forces.

In addition, such a position would have a significantly negative impact on digital advertising for publishers and frustrate the ability of advertisers to reach young, independent consumers.

Finally, it is not clear on what basis the WP29 recommends that, wherever possible, controllers should not rely upon the exceptions provided in Article 22 to justify the application of automated decision-making mechanism to children. Reference to recital 71 providing that such measures should not concern a child is not sufficient.

The enormous breadth of uses of automated decision-making and profiling in various sectors

It is useful that the 'Introduction' of the guidelines aims to provide an overview of how automated decision-making and profiling are used in practice. However, it is difficult to fully understand and describe the enormous breadth of uses of automated decision-making and profiling in the various sectors. We note here a few examples in order to assist WP29 in its understanding of how complex it can be to apply the general legal provisions to such different uses.

Here are some examples of how automated decision-making and profiling are used today in various sectors:

- In the **banking sector**, credit card fraud detection and prevention as well as creation of predictive models to analyse risk and create a single view of the risk and exposure across all entities of a banking group.
- Predicting risk, and, identification of fraud and other criminal activities within the insurance sector in order to drive down claims and costs to the insurer, savings which can be passed to the consumer.
- Detection of medical conditions and trends by **pharmaceutical companies**.
- Service improvement, product customization and supply management, product placement and marketing campaign improvement as well as warranty management in the **retail sector**.

- Determination of effectiveness of website architecture, services improvement, customer relationship management, personalisation of services and products in **e-commerce**.
- Decision support analytics systems in the **airline sector** to ensure efficiency and competitiveness.
- In the **telecommunications sector**, improvement of marketing campaigns and customer retention programs.
- Detection and prevention of discrimination in **employment, housing or academic decisions** which may be influenced by human nature either intentionally or unintentionally.
- Identification and mitigation of network-connected devices which are infected by, and/or distributing malware or other **cybersecurity** threats, or which behave in ways that are indicative of cybercriminal activity or misuse;
- In the **Internet enabled world**, machine learning and artificial intelligence to e.g. create better spell checkers, improve translation services, enable traffic prediction, ensure content availability, design and deplore disaster recovery programs and enable connected cars.
- Management of smart meters, consumption and demand forecasting in the **energy sector**.