



IN THIS ISSUE

PG. 2

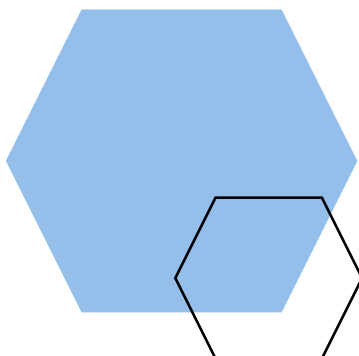
Ethics of AI

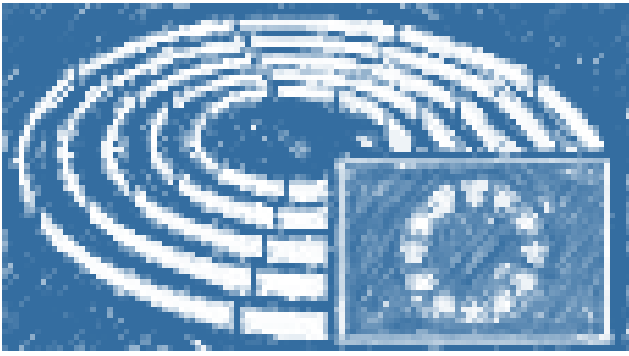
PG. 4

National DPAs Guidance

PG. 6

Enforcement





EUROPEAN PARLIAMENT RELEASES GUIDELINES ON ETHICS IN AI

EU guidelines on ethics in artificial intelligence:
Context and implementation available [here](#)

THE INFORMATION COMMISSIONER'S OFFICE (ICO) HAS OPENED AN INVESTIGATION FOLLOWING MEDIA REPORTS ON FACIAL RECOGNITION TECHNOLOGY BEING USED WITHIN SECURITY CAMERAS IN THE KING'S CROSS AREA OF LONDON

The discussion around artificial intelligence (AI) technologies and their impact on society is increasingly focused on the question of whether AI should be regulated. Following the call from the European Parliament to update and complement the existing Union legal framework with guiding ethical principles, the EU has carved out a 'human-centric' approach to AI that is respectful of European values and principles. As part of this approach, the EU published its guidelines on ethics in AI in April 2019, and European Commission President-elect, Ursula von der Leyen, has announced that the Commission will soon put forward further legislative proposals for a coordinated European approach to the human and ethical implications of AI. Against this background, this paper aims to shed some light on the ethical rules that are now recommended when designing, developing, deploying, implementing or using AI products and services in the EU. Moreover, it identifies some implementation challenges and presents possible further EU action ranging from soft law guidance to standardisation to legislation in the field of ethics and AI. There are calls for clarifying the EU guidelines, fostering the adoption of ethical standards and adopting legally binding instruments to, inter alia, set common rules on transparency and common requirements for fundamental rights impact assessments, and to provide an adequate legal framework for face recognition technology. Finally, the paper gives an overview of the main ethical frameworks for AI under development in countries such as the United States and China.



Full paper available [here](#)

OECD GOOD PRACTICE GUIDE ON CONSUMER DATA

This paper aims to complement the OECD Recommendation of on Consumer Protection in E-Commerce and discuss consumer policy issues associated with consumer data practices, offering greater insights into how consumer protection authorities can and have applied the principles in the Recommendation to address those issues. The guide focuses on selected consumer data practices, including: i) deceptive representations about consumer data practices; ii) misrepresentations by omission; and iii) unfair consumer data practices. It then provides key business tips to comply with consumer protection principles under the E-commerce Recommendation.

NATIONAL DPAs GUIDANCE



Full guidance available [here](#)

SPAIN: AEPD PUBLISHES LIST OF PROCESSING ACTIVITIES NOT REQUIRING A DPIA

IN ORDER TO ASSIST CONTROLLERS IN IDENTIFYING THE KINDS OF DATA-PROCESSING THAT DO NOT REQUIRE A DPIA, THE GDPR PROVIDES THAT SUPERVISORY AUTHORITIES MAY PUBLISH A LIST SETTING OUT WHAT KIND OF PROCESSING DOES NOT REQUIRE A DPIA. THIS LIST SHALL BE NOTIFIED TO THE EUROPEAN DATA PROTECTION BOARD (EDPB).

A DPIA is a costly process and the principle of economy of means must be applied. As such, an initial qualitative analysis may conclude that no DPIA is necessary. In this case, such a decision must have enough grounds. Obviously, this obligation does not extend to the processing of data that are not of a personal nature. Although, as a precautionary measure in order to protect the rights of citizens, the concept of 'personal data' established in the GDPR must be considered extensively, i.e. the default assumption should be that the data being processed are of a personal nature, and it should not be assumed a priori that the data being processed do not fall into this category. The following list establishes the forms of data-processing that are exempt from carrying out a DPIA without prejudice to any other obligation stipulated by GDPR and, consequently, this does not mean that they are exempt from the duties laid down in the GDPR framework that governs personal data-processing. This list is based on the document WP 2481 and complements its criteria in order to help data controllers to understand data processing that do not require DPIA.

DUTCH RADIOCOMMUNICATIONS AGENCY (AT) ISSUES REPORT ON IOT DEVICE SECURITY

The 'Internet of Things' is growing fast. The devices are developed with a view to new functionalities, with relatively little attention being paid to security and privacy. Many examples are known of security incidents caused by unsafe IoT devices.

In order to gain insight into the current state of the protection of IoT consumer devices, the Telecom Agency has investigated the digital protection of these devices.

Full report is available [here](#)

DENMARK: DPA CHANGES PRACTICE ON PUBLISHING PHOTOS OF IDENTIFIABLE PERSONS ON THE INTERNET

The Danish Data Protection Agency is changing its practice in relation to publishing images on the Internet. Since 2002, it has been the practice of the Danish Data Protection Agency that the assessment of whether images can be published on the Internet varies according to whether it is a situation picture or a portrait picture.

Situational images are images where an activity or situation is the real purpose of the image, such as photos of the audience for a concert. The contradiction to this is portrait pictures, the purpose of which is to depict one or more specific persons.

Where publication of situational images on the Internet could normally have taken place without the persons in the image being allowed to do so, the Danish Data Protection Agency has, as a starting point, required consent to the publication of portrait images.

However, the Danish Data Protection Agency has received several inquiries regarding the practice of the supervision, including the distinction between situational and portrait images, which has given the Authority reason to consider the current practice.

In the EDPS's view, it is in particular the demarcation between situational and portrait images that has in practice proved to be unclear. Furthermore, the technological and societal development that has taken place since 2002 has led to a significant shift in the use of the Internet. Pictures of identifiable persons are thus widely published today on websites and social media such as Facebook and Instagram. Many people perceive this to be quite unproblematic as long as there is the publication of completely harmless pictures of them on the internet.

Against this background - and after discussion in the Data Council - the Danish Data Protection Agency has decided to change its practice. The Danish Data Protection Agency will no longer distinguish between situational and portrait images, and in future it will be the opinion of the Danish Data Protection Agency that the question whether a picture can be published on the Internet - without the consent of the person concerned - will depend on a comprehensive assessment of the picture and the purpose of the publication. . It is therefore the responsibility of the data controller - as with any processing of personal data - to assess the basis on which a picture of an identifiable person can be published.

[Read more in the Danish Data Protection Agency's text on publishing images on the Internet](#) .

ENFORCEMENT

POLISH DPA IMPOSES €645,000 FINE FOR INSUFFICIENT ORGANISATIONAL AND TECHNICAL SAFEGUARDS

THE PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE IMPOSED A FINE OF AN AMOUNT HIGHER THAN PLN 2.8 MILLION (CA. 645,000 EUROS) ON MORELE.NET.

The company's organisational and technical measures for the protection of personal data were not appropriate to the risk posed by the processing of personal data, which means that data of about 2.2 million people have fallen into the wrong hands. There was a lack of appropriate response procedures to deal with the emergence of unusual network traffic, concluded the President of the Personal Data Protection Office (UODO).

While imposing the fine, the supervisory authority concluded that the breach which took place in this case was of considerable importance and of serious character, and concerned a large number of persons. In its decision, the supervisory authority also pointed out that, as a result of the infringement, there was a high risk of adverse effects on persons whose personal data fell into the wrong hands, such as identity theft.

The data concerned included: name and surname, phone number, email, delivery address. However, in the case of about 35,000 people, the data leaked from their installment loan application. The scope of the data comprised the personal ID number (PESEL number), the series and the number of the identity document, educational background, registered address, correspondence address, source of income, amount of net income, the cost of living of the household, marital status, as well as the amount of credit commitments or maintenance obligations.

In the decision imposing the fine, the President of UODO concluded that the company by failing to comply with the required technical means of data protection, has breached, inter alia, the principle of confidentiality, as set out in Article 5 (1)(f) of the GDPR. Therefore, there has been unauthorised access to and obtaining of customers' data. The authority considered that unsuccessful measures for the authentication of data access were put in place. The company had implemented additional technical security measures after the breach.

The investigation revealed that the infringement occurred also because of ineffective monitoring of potential risks. The investigation further revealed other misconduct, but it was the lack of appropriate technical (insufficient safeguards) and organisational measures (on the monitoring of potential risks related to atypical online behaviour) that led to imposing a fine. In determining its amount, however, the President of UODO took account of mitigating circumstances, such as: action taken by the company to put an end to the infringement, good cooperation with the controller and the fact that the company has not breached the personal data protection law before.

To read the full press release in Polish, click [here](#)

The Polish text of the decision is available [here](#)

THE BELGIAN DATA PROTECTION AUTHORITY IMPOSES A FINE OF €10,000

THE BELGIAN DATA PROTECTION AUTHORITY IMPOSED A FINE OF €10,000 ON A MERCHANT FOR THE DISPROPORTIONATE USE OF THE ELECTRONICAL IDENTITY CARD FOR THE PURPOSE OF CREATING A LOYALTY CARD.

The Authority has sanctioned a merchant who offers as a sole means of creating a loyalty card the reading of the electronic identity card. The administrative fine imposed amounts to € 10,000. The electronic identity card contains a lot of information about the cardholder and the use of this data, without the client's consent, is considered disproportionate to the proposed service.

Narrative: reading the eID in exchange for a loyalty card

APD has received a complaint about a merchant's use of the electronic identity card (eID) as part of a commercial service, namely the creation of a loyalty card. Since the complainant did not want to present his identity card, he was refused the loyalty card, but he offered to send the merchant's data in writing in order to be able to benefit from a loyalty card. The APD Litigation Chamber found this practice to be in breach of the General Data Protection Regulation (GDPR) for a number of reasons.

Non-compliance with the data minimization principle

The principle of minimization is an important principle in the GDPR that requires data controllers to limit the amount of personal data collected as well as the retention period of the data to what is strictly necessary in view of the purpose.

For the creation of the loyalty card, the merchant requires to read data on the eID such as name, first names, address, etc., but he also wants to access the photo and barcode that is linked to the national registry number. The Litigation Chamber recalls that the national registry number is a data subject to strict rules regarding its consultation and use.

The Litigation Chamber therefore considers that the reading and use of all the data present on the electronic identity card in a commercial setting are disproportionate data processing with regard to the objective of creating a loyalty card.

Absence of valid consent

A processing of personal data, to be lawful, must be based on one of the six legal bases provided by the RGPD. The trader invokes the consent as a legal basis to justify the processing of the data taken from the customer's eID but the Contentious Chamber disputes the validity of this legal basis.

To be valid, a consent must be free, specific and informed. The Litigation Chamber considers that the consent given in this case can not be considered freely given consent as no alternative is offered to clients. If customers refuse to use their electronic identity card for the creation of a loyalty card, they are penalized and can not enjoy benefits and discounts because no alternative is offered.

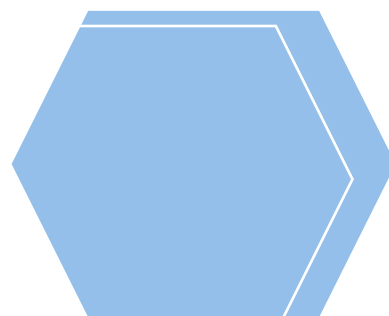
Translation by Google. You can read the press release [here](#) in Fench and [here](#) in Dutch

UK LEADS INTERNATIONAL EFFORT TO TRACK VALUE OF OFFICIAL DATA

UK – THE OFFICE FOR NATIONAL STATISTICS (ONS) HAS BEGUN WORK TO LEAD A UN PROJECT THAT AIMS TO DEFINE AND MEASURE THE VALUE OF GLOBAL STATISTICS.

On September 24th organisations from around the world will gather in London to attempt to track the monetary value of metrics such as gross domestic product (GDP), migration and trade statistics. The event follows a set of recommendations published by the United Nations Economic Commission for Europe (UNECE) from a UK-led international task force.

Katie McQuater for ResearchLive has the [full story](#)



NIELSEN PARTNERS WITH OXFORD ON IMAGE RECOGNITION

US – NIELSEN AND THE UNIVERSITY OF OXFORD HAVE TEAMED UP ON A PROJECT THAT AIMS TO BOOST IMAGE RECOGNITION OF CONSUMER-PACKAGED GOODS PRODUCTS IN STORES.

Oxford's Visual Geometry Group, led by professors Andrew Zisserman and Andrea Vedaldi, will work with Nielsen's Image Recognition Group to more precisely and quickly identify in-store products based on Nielsen's product reference data.

The researchers will build on the eCollection tool's algorithms using advanced deep learning, which Nielsen expects will improve accuracy and reduce the costs of its product identification and classification.

Katie McQuater for ResearchLive has the [full story](#)

CONSUMER RESEARCH – HOW EU CITIZENS PERCEIVE DIGITAL ADVERTISING SINCE GDPR

EDAA PUBLISHED THE RESULTS OF ITS LATEST CONSUMER RESEARCH ON PERCEPTIONS AND ATTITUDES TOWARDS DIGITAL ADVERTISING POST-GDPR.

This consumer research was conducted in March 2019 in France, Germany, Poland, Spain & the UK to **explore consumer attitudes and perceptions towards online advertising and determine how these may have changed since the introduction of GDPR**. The research results are informing EDAA's assessment of shifts in consumer perspectives as it looks to further develop the industry's self-regulatory programme for the benefit of consumers and industry alike.

The research infographic can be viewed and downloaded [here](#).

Full article available [here](#).

MICROSOFT AND HARVARD TO DEVELOP PRIVACY PLATFORM

US – MICROSOFT HAS PARTNERED WITH HARVARD UNIVERSITY'S INSTITUTE FOR QUANTITATIVE SOCIAL SCIENCES TO BUILD AN OPEN SOURCE PLATFORM FOR RESEARCHERS WHERE DATA CAN BE SHARED PRIVATELY.

The partnership will draw on differential privacy, a technology used to extract insights from data sets containing personal information while protecting data privacy.

Katie McQuater for ResearchLive has the [full story](#)

FACEBOOK TO BUY BRAIN INTERFACE FIRM

[FACEBOOK INC.](#) AGREED TO ACQUIRE [CTRL-LABS](#), A TECHNOLOGY STARTUP THAT IS BUILDING SOFTWARE TO LET PEOPLE CONTROL A DIGITAL AVATAR USING ONLY THEIR THOUGHTS.

The world's largest social network is paying between \$500 million and \$1 billion, according to people familiar with the deal.

The closely held four-year-old startup, which has dozens of employees and has raised tens of millions in venture capital, uses a bracelet to measure neuron activity in a subject's arm to determine movement that person is thinking about, even if they aren't physically moving. That neuron activity is then translated into movement on a digital screen. Facebook declined to comment on the price of the acquisition.

Bloomberg has the full story [here](#)

