GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Having convened today, in the presence of Mr. Antonello Soro, President, Ms. Augusta Iannini, Vice-President, Ms. Giovanna Bianchi Clerici and Prof. Licia Califano, Members, and Mr. Giuseppe Busia, Secretary General;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter 'GDPR');

Having regard to, in particular, Article 35(1) of the GDPR, providing for the controller's obligation to carry out, prior to the processing, an assessment of the impact of the processing where such processing '*in particular using new technologies, and taking into account the nature, scope, context and purposes [of the processing]*' is likely to result in a high risk to the rights and freedoms of natural persons;

Having regard to paragraph 3 of the aforementioned Article, which sets out cases where a data protection impact assessment is required;

Having regard to Article 35(10), which lays down cases where the above assessment is not required, namely '*Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, […] unless Member States deem it to be necessary to carry out such an assessment prior to processing activities*';

Whereas Article 35(4) requires national supervisory authorities to establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment, and to communicate such list to the European Data Protection Board referred to in Article 68 of the GDPR;

Whereas Article 35(6) provides that the consistency mechanism referred to in Article 63 of the GDPR shall be applied by the competent supervisory authority where the aforementioned list involves '*processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union';*

Having regard to the considerations made in Recitals No. 71, 75 and 91 of the GDPR;

Having regard to the 'Guidelines on data protection impact assessment and determining whether processing "is likely to result in a high risk" for the purposes of Regulation (EU) 2016/679' issued by the Article 29 Working Party on 4 April 2017 as subsequently amended and adopted on 4 October 2017 and thereafter endorsed by the European Data Protection Board on 25 May 2018 (hereinafter 'WP 248, rev. 01'), which established the following nine criteria to be taken into account with a view to determining whether processing is likely to result in a 'high risk' – namely, 1) evaluation or scoring, including profiling and predicting, especially from '*aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements*'; 2) automated decision-making with legal or similar significant effect on natural persons; 3) systematic monitoring of data subjects; 4) sensitive data or data of a highly personal nature; 5) data processed on a large scale; 6) matching or combining datasets; 7) data concerning vulnerable data subjects; 8) innovative use or applying new technological or organisational solutions; 9) when the processing in itself '*prevents data subjects from exercising a right or using a service or a contract*' ;

Noting that a processing activity meeting two or more of the above criteria is likely to result in a high risk to the rights and freedoms of the data subjects and requires, accordingly, a data protection impact assessment to be carried out (see WP 248, rev. 01, p. 11);

Whereas the Garante has established a list of the kind of processing operations under Article 35(4) that are subject to a data protection impact assessment;

Whereas the provisions set out in Article 35(1) of the GDPR whereby '*where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the*

processing, carry out an assessment of the impact of the envisaged processing on the protection of personal data' shall prevail in all cases;

Whereas the aforementioned list was established on the basis of WP248, rev. 01, in order to specify and supplement the relevant contents thereof;

Noting that the aforementioned list was communicated to the European Data Protection Board on 11 July 2018 to obtain the required opinion (see Art. 35(4) and (6), and Art. 64(1), letter a), of the GDPR);

Having regard to the considerations made by the European Data Protection Board in its opinion as adopted on 25 September 2018 and notified on 2 October 2018 (available on *https://edpb.europa.eu*);

Having resolved, pursuant to Article 64(7) of the GDPR, to abide by the considerations contained in the aforementioned opinion, amend the relevant draft decision accordingly, and communicate this to the Chair of the Board;

Noting that the aforementioned list only relates to the kind of processing operations that are subject to the consistency mechanism and is not exhaustive, which is without prejudice accordingly to the obligation to carry out a data protection impact assessment if two or more of the criteria established by the WP248, rev. 01, are met, and that in some cases '*a data controller can consider that a processing meeting only one of [the aforementioned] criteria requires a data protection impact assessment*' (see WP248, rev. 01, p. 11);

Noting additionally that the aforementioned list may be amended or supplemented further also based on the outcome of the initial implementing phase of the GDPR;

Having regard to the considerations made by the Secretary General pursuant to Article 15 of the Rules of Procedure of the Garante, No. 1/2000;

Acting on the report submitted by Mr. Antonello Soro;

BASED ON THE ABOVE PREMISES,

a) Establishes the list of the kind of processing operations, which are subject to the consistency mechanism, for which a data protection impact assessment is required pursuant to Article

35(4) and Article 57(1), letter k), of the GDPR, without prejudice to the aforementioned WP248, rev. 01, such processing operations being reported in Annex No. 1 which shall be an integral part hereof and specifying the guidance contained in the aforementioned WP248, rev. 01;

b) Communicates this decision, which has been amended in accordance with the considerations made in the opinion as per the premises hereof, to the Chair of the European Data Protection Board pursuant to Article 64(7) of the GDPR;
c) Forwards a copy of this decision to the Ufficio pubblicazione leggi e decreti [Publishing department for laws and decrees] of the Ministry of Justice with a view to its publication in the Official Journal of the Italian Republic.

Done in Rome, on the 11th day of the month of October 2018

THE PRESIDENT

THE RAPPORTEUR

THE SECRETARY GENERAL

Attachments: 1

Annex No. 1

1.	Large-scale processing activities for assessment or scoring purposes and processing activities that entail profiling of data subjects and the performance of predictive activities, also online or via apps, relating to '*aspects concerning a data subject's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*'.
2.	Automated processing aimed at taking decisions that produce '*legal effects*' on the data subject or '*similarly significantly affect*' a data subject, including any decisions that prevent a data subject from exercising a right or using a good or service or continuing to be party to an existing contract – for instance, screening of bank customers by way of the data held by a credit bureau.
3.	Processing entailing a systematic use of data to observe, monitor or control data subjects including data collection via networks, also online or via apps, and the processing of unique identifiers capable to identify users of information society services including web services, interactive TV, etc. as related to usage and viewing habits over a long time span. This includes processing of metadata e.g. in the telecommunications, banking, etc. sectors as performed not only for profiling, but more generally for organisational purposes, to provide budgetary estimates, for technological upgrades, network improvement reasons, provision of anti-fraud and/or anti-spam services, for security purposes, etc.
4.	Large-scale processing of highly personal data including, *inter alia*, data relating to an individual's private life or household (such as electronic communications data, whose confidentiality must be preserved) or data impacting the exercise of fundamental rights (such as location data, whose collection challenges freedom of movement), or any data whose breach can substantially affect the data subject's daily life (such as financial data, which might be used to commit payment-related fraud).
5.	Processing carried out in connection with the employer-employee relationship by way of technological systems (including video surveillance and geolocation systems) enabling the distance monitoring of employees' activities (see the guidance provided in WP248, rev. 01, with regard to criteria No. 3, 7, and 8).
6.	Non-occasional processing of data relating to vulnerable individuals (children, persons with disabilities, the elderly, mentally unsound

	individuals, patients, asylum applicants).
7.	Processing carried out with the help of innovative technologies including the use of particular organisational measures (for instance, IoT-related processing activities, AI systems, use of online voice assistants via voice and text scanning, monitoring performed by wearable devices, proximity tracking such as in the case of wi-fi tracking) whenever at least one additional criterion is met out of those set out in WP248, rev. 01.
8.	Processing entailing the large-scale exchange of data among data controllers via electronic networks.
9.	Processing of personal data that is carried out by linking, combining or matching information including processing that envisages the matching of digital goods usage data with payment data (e.g. with regard to mobile payment solutions).
10.	Processing of special categories of personal data under Article 9 of the GDPR or of data relating to criminal convictions and offences under Article 10 of the GDPR, where such data are linked with other personal data that have been collected for different purposes.
11.	Systematic processing of biometric data by taking account, in particular, of the amount of the data, the duration or persistence of the processing activity.
12.	Systematic processing of genetic data by taking account, in particular, of the amount of the data, the duration or persistence of the processing activity.

PLEASE NOTE * for the sake of clarification, that wording like 'systematic' and 'non-occasional' as used in the DPIA lists (items 6, 11, and 12) is to be traced back to the 'large scale' criterion pursuant to the considerations made in document WP248rev.1 (p. 11):

'5. Data processed on a large scale: the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
a. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
b. the volume of data and/or the range of different data items being processed;

c. the duration, or permanence, of the data processing activity;
d. the geographical extent of the processing activity.'

Furthermore, the wording 'biometric data' in item 11 of the DPIA List is to be understood as 'biometric data, processed for the purpose of uniquely identifying a natural person'.

** Clarification posted on the website page addressing the DPIA procedures and list, which can be reached from all the sections of our website where such list is published*