

“ABC” OF THE GDPR

‘Accuracy’ – one of the principles relating to processing of personal data, which entails that personal data always have to be accurate and kept up to date where necessary.

‘Board (“EDPB)” – the European Data Protection Board, the EU body that supervises the implementation and enforcement of the GDPR.

‘Consent’ – the freely given, specific, informed and unambiguous indication of the data subject’s wishes or a clear affirmative act whereby the data subject accepts the processing.

‘Controller’ – the entity that determines the purposes and means for the processing of personal data.

‘Data breach’ – the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data resulting from a breach of security; a data breach must be reported within established periods to the supervisory authority and the data subjects.

‘Data protection impact assessment (“DPIA”) – the evaluation of the impact of the envisaged processing operations prior to the start of the actual processing; this is only necessary in high risk situations (e.g. in the case of new technology or a profiling operation with significant consequences for the data subjects).

‘Data protection officer (“DPO”) – the person (internal or external) who supervises compliance with the GDPR and has the necessary knowledge, resources and authority to do so; a DPO is, amongst other things, obligatory if the processor regularly and systematically processes personal data on a large scale or if the processor processes special categories of personal data.

‘Data subject’ – the individual to whom the personal data relate.

‘GDPR’ – the abbreviation for “*General Data Protection Regulation*”.

‘Lawfulness’ – the principle according to which personal data may only be processed if a valid legal ground exists for doing so (e.g. consent of the data subject, execution of an agreement or the pursuit of a legitimate interest of the controller).

‘(Lead) supervisory authority (“DPA” or “SA”) – the national authority that is responsible for monitoring the application of the GDPR; the supervisory authority of the main place of establishment of the controller or processor is competent to act as lead supervisory authority for cross-border processing by this controller or processor (“*one-stop-shop principle*”).

‘Personal data’ – any information relating to an identified or identifiable natural person, including indirect identification, such as a name, an identification number, location data, IP address or factors that are specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

‘Processing’ – any action with, or operation performed on personal data, whether or not automated.

‘Processor’ – the entity that processes personal data on behalf of the controller.

‘Profiling’ – automated processing of personal data for the evaluation of information relating to a person or in order to analyse or predict her behaviour (e.g. performance at work, economic situation, health, location or personal preferences).

‘Purpose limitation’ – the principle according to which personal data may only be processed for specified, explicit and legitimate purposes; the personal data must be limited to what is necessary for these purposes (“data minimisation”) and may only be kept for as long as it is necessary for the intended purpose.

‘Records of processing activities’ – the records that contain specific information about the processing activities (e.g. purposes, data subjects, personal data, recipients and transfers) which take place under the responsibility of the controller; each controller must maintain such records.

‘Rights of the data subject’ – the rights that the GDPR provides for data subjects, such as the right to information and access to personal data, rectification and erasure of the data, objection to direct marketing practices, objection to automated decision-making and profiling and portability of the data.

‘Special categories of personal data’ – personal data which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic or biometric data, data concerning health or a person’s sex life or sexual orientation; in principle, the processing of these personal data is prohibited.

‘Transfers’ – the transmission of personal data to a country outside of the European Economic Area (or to an international organisation); such transfer is only possible if done in accordance with the provisions of the GDPR (e.g. if an adequacy decision is present).

‘Sanctions’ – liability for material and immaterial damage and administrative fines up to 20,000,000 EUR or up to 4% of the total worldwide annual turnover of the involved company in the preceding financial year, if this figure is higher.

For further questions / information: Anouk Focquet – anouk.focquet@contrast-law.be