STATUTORY INSTRUMENTS

2014 No. 3141

The Criminal Justice and Data Protection (Protocol No. 36) Regulations 2014

PART 4

Data Protection in relation to Police and Judicial Cooperation in Criminal Matters

CHAPTER 2

Duties of competent authorities and rights of data subjects

Duties of competent authorities

29. When undertaking activities in relation to the processing of personal data to which this Part applies, a UK competent authority must comply with regulations 30 to 42, 43(2), 44, 45, 47 and 48.

Principles of lawfulness, proportionality and purpose

30.—(1) Personal data must be—

(a) processed lawfully;

(b) collected only for specified, explicit and legitimate purposes;

(c) processed only for the purposes for which the data were collected;

(d) adequate, relevant and not excessive in relation to the purposes for which they were collected.

(2) Further processing of personal data may only be undertaken—

(a) for historical, statistical or scientific purposes, if the relevant conditions are complied with;

(b) for any other purpose, if—

(i) the processing is not incompatible with the purposes for which the data were collected;

(ii) the competent authority is permitted by law to carry it out; and

(iii) the processing is necessary and proportionate to that other purpose.

(3) When undertaking further processing for historical, statistical or scientific purposes, consideration must be given to whether the purpose can be achieved by making the data anonymous.

Rectification, erasure and blocking

31.—(1) A UK competent authority must—

(a) rectify personal data which are inaccurate;

(b) complete or update personal data where that is possible and necessary;

(c) erase personal data or make them anonymous where they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed.

(2) Nothing in paragraph (1)(c) precludes a competent authority from archiving the data in a separate dataset for an appropriate period in accordance with an enactment or rule of law.

(3) Personal data must be blocked instead of erased if the competent authority has reasonable grounds to believe that erasure could affect the legitimate interests of the data subject and, once blocked, that data shall be processed only for the purpose which prevented their erasure.

(4) When the personal data are contained in a judicial decision or record related to the issuance of a judicial decision, rectification, erasure or blocking is permitted only where it complies with an enactment or rule of law regarding judicial proceedings.

(5) A competent authority which refuses to rectify, erase or block data under paragraph (1), having been asked by the data subject to do so, must give notice of its decision in writing to the data subject within a reasonable period of making it.

(6) That notice must inform the data subject that they may make a complaint about the refusal to the Commissioner.

(7) The Commissioner must examine any such complaint and, having done so, inform the data subject of whether or not the competent authority acted properly.

(8) If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, that item may be marked for the purpose of indicating that its accuracy or inaccuracy cannot be ascertained.

Establishment of time limits for erasure and review

32. A UK competent authority must—

(a) establish time limits for the periodic review of the need for continued storage of personal data and for its erasure; and

(b) ensure that those time limits are observed.

Processing of sensitive personal data

33. Sensitive personal data may be processed only if—

(a) necessary; and

(b) at least one of the conditions in Schedule 3 to the Act (conditions relevant for the processing of sensitive personal data), with the exception of the condition in paragraph 8 of that Schedule, is satisfied.

Automated individual decisions

34.—(1) A decision which produces an adverse legal effect for the data subject or significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted where it aids the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

(2) A UK competent authority which proposes to make a decision permitted by paragraph (1) must take steps to safeguard the legitimate interests of the data subject (for example, by allowing them to make representations).

Verification of quality of data that are transmitted or made available

35.—(1) A UK competent authority must take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up-to-date are not transmitted or made available.

(2) Where a UK competent authority transmits or makes available personal data it should, as far as practicable, verify the quality of personal data before transmitting it or making it available.

(3) Where a UK competent authority transmits or makes available personal data, it must, as far as possible, add available information which enables the recipient to assess the degree of accuracy, completeness and reliability of the data, including whether they are up-to-date.

(4) If personal data are transmitted or made available to a competent authority without that authority having requested them, that authority must verify without delay whether the data are necessary for the purpose for which they were transmitted.

(5) This paragraph applies where a UK competent authority transmits or makes available personal data to a non-UK competent authority and it becomes apparent that the transmitted data—

(a) are incorrect; or

(b) have been unlawfully transmitted.

(6) Where paragraph (5) applies, the UK competent authority must without delay—

(a) notify the recipient of the inaccuracy or unlawful transmission; and

(b) rectify, erase or block the data in accordance with regulation 31.

Time limits

36.—(1) A UK competent authority transmitting or making available personal data to a non-UK competent authority or to a UK competent authority referred to in Part 2 of Schedule 4 must when doing so notify the recipient of the time limits established for its retention.

(2) If—

(a) a non-UK competent authority transmits or makes available data to a UK competent authority that is subject to the Data Protection Framework Decision; and

(b) when doing so, indicates a time limit for the retention of that data,

the UK competent authority must take steps on the expiry of that time limit to erase or block the data, or review whether they are still needed.

(3) The obligation in paragraph (2) does not apply if, on the expiry of the time limit, the data are required for a current investigation, the prosecution of a criminal offence or enforcement of a criminal penalty.

(4) If a non-UK competent authority transmits or makes available data to a UK competent authority that is subject to the Data Protection Framework Decision without indicating a time limit for its retention, the UK competent authority shall apply any relevant time limits provided for under any enactment or rule of law.

Logging and documentation

37.—(1) Any transmission of personal data by a UK competent authority must be logged or documented by that authority for the purposes of verifying the lawfulness of the processing and self-monitoring, and ensuring proper data integrity and security.

(2) A log or documentation prepared under paragraph (1) must be sent on request to the Commissioner, who may use the information only for the control of data protection and for ensuring proper data processing as well as data integrity and security.

Processing of personal data received from or made available by an authority in another Member State

38.—(1) A UK competent authority may only process personal data received from or made available by a non-UK competent authority for the purpose for which they were transmitted or made available, or for any of the following purposes—

(a) the prevention, investigation, detection or prosecution of a criminal offence, or the execution of a criminal penalty, other than that for which the data were transmitted or made available;

(b) other judicial and administrative proceedings directly linked to the prevention, investigation, detection or prosecution of a criminal offence or execution of a criminal penalty;

(c) prevention of an immediate and serious threat to public security;

(d) any other purpose only with the prior consent of the transmitting authority or the data subject's consent given in accordance with national law.

(2) A UK competent authority may undertake further processing of personal data for historical, statistical or scientific purposes if the relevant conditions are complied with.

(3) When undertaking further processing for historical, statistical or scientific purposes, consideration must be given to whether the purpose can be achieved by making the data anonymous.

Compliance with national processing restrictions

39.—(1) Where a non-UK competent authority—

(a) transmits or makes available data to a UK competent authority in accordance with the Data Protection Framework Decision; and

(b) notifies the UK competent authority of specific processing restrictions that would apply in the specific circumstances under the law of its Member State to the exchange of that data had it been made within that State,

the UK competent authority shall comply with those restrictions.

(2) Where—

(a) a UK competent authority transmits or makes available data to a non-UK competent authority in accordance with the Data Protection Framework Decision; and

(b) in the specific circumstances, the exchange of that data would have been subject to specific processing restrictions by virtue of or under any enactment or rule of law had it been made to another UK competent authority,

the UK competent authority shall notify the recipient of those restrictions.

(3) The restrictions referred to in paragraphs (1) and (2) are limited to those applying under the law of the Member State of the competent authority transmitting or making available the data to such exchanges of data between competent authorities within that State.

Transfer to competent authorities in third countries or to international bodies

40.—(1) Personal data transmitted or made available to a UK competent authority by a non-UK competent authority may be transferred to a third country or an international body only if—

(a) it is necessary for the prevention, investigation, detection or prosecution of a criminal offence or the execution of a criminal penalty;

(b) the receiving authority in the recipient third country or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(c) subject to paragraph (2), the competent authority from which the data were obtained has given its prior consent to the transfer in compliance with the applicable national law; and

(d) subject to paragraph (3), the third country or international body concerned ensures an adequate level of protection for the intended data processing.

(2) Transfer without prior consent is permitted only if—

(a) transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third country or to essential interests of a Member State; and

(b) such consent cannot be obtained in good time.

(3) Where a transfer is made without prior consent, the authority otherwise responsible for giving it must be informed without delay.

(4) Paragraph (1)(d) does not apply where—

(a) the transfer is necessary to pursue—

(i) the legitimate specific interests of the data subject; or

(ii) other legitimate prevailing interests, especially important public interests; or

(b) the third country or receiving international body provides safeguards which are deemed adequate by the person or body that intends to make the transfer.

(5) The adequacy of the level of protection referred to in paragraph (1)(d) shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations including, in particular—

(a) the nature of the data;

(b) the purpose and duration of the proposed processing operation or operations;

(c) the State of origin and the State or international body of final destination of the data;

(d) the rules of law in force in the third country or which apply to the international body in question; and

(e) the professional rules and security measures which apply.

(6) In this regulation, "third country" means a State other than a Member State.

Transmission to private parties

41.—(1) A UK competent authority may transmit to a private party personal data received from or made available to it by a non-UK competent authority only if—

(a) the authority from which the data were obtained has consented in compliance with the applicable national law to its transmission;

(b) no legitimate specific interests of the data subject prevent transmission; and

(c) in the particular case, transmission by the UK competent authority is essential for—

(i) performance of a task lawfully assigned to it;

(ii) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(iii) prevention of an immediate and serious threat to public security; or

(iv) prevention of serious harm to the rights of individuals.

(2) The UK competent authority transmitting the data to a private party shall inform the private party of the purposes for which the data may exclusively be used.

(3) In this regulation, "private party" does not include a body which exercises functions of a public nature, whether under contract or otherwise, when engaging in an activity that involves the exercise of those functions.

Information on request of the competent authority

42. The recipient of any data transmitted or made available by a UK competent authority shall, on request by that authority, inform it about their processing of that data.

Information for the data subject

43.—(1) A data subject must be informed regarding the collection or processing of personal data by a UK competent authority in accordance with national law.

(2) A UK competent authority to which personal data have been transmitted or made available by a non-UK competent authority must not inform the data subject of that fact without the prior consent of the non-UK competent authority.

Right of access

44.—(1) Sections 7 (right of access to personal data), 8 (provisions supplementary to section 7) and 67 (orders, regulations and rules) of the Act apply in relation to the processing of personal data to which this Part applies, with the following modifications.

(2) Section 7 shall have effect as if—

(a) a reference to a "data controller" were a reference to a "UK competent authority" within the meaning of regulation 27(1);

(b) in subsection (1)—

(i) the references to sections 9 and 9A of the Act were omitted; and.

(ii) in paragraph (d), the words between "relating to him" and "has constituted or is likely to constitute" were omitted;

(c) after subsection (4) there was inserted—

"(4A) Subsection (1) does not require a UK competent authority to provide any information if, having due regard to the legitimate interests of the person concerned, refusal to do so is a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security; or

(e) protect the data subject or the rights and freedoms of others.

(4B) Where a UK competent authority refuses to provide information or restricts access to it in response to a request made under subsection (1), the authority must give the data subject written notice of its decision, which must also set out—

(a) except where a reason under subsection (4A) exists, the factual or legal reasons on which the decision is based; and

(b) notice of the data subject's entitlement to appeal to the Commissioner or to a court."; and

(d) subsection (12) were omitted.

(3) Section 8 shall have effect as if—

(a) a reference to a "data controller" were a reference to a "UK competent authority" within the meaning of regulation 27(1); and

(b) subsection (5) were omitted.

Right to compensation

45.—(1) An individual who suffers damage by reason of any contravention by a UK competent authority of any of the requirements of this Part is entitled to compensation from that authority—

(a) for that damage; and

(b) for any distress suffered in addition to that damage.

(2) In proceedings brought by virtue of paragraph (1), it is not a defence to prove that any data transmitted or made available were inaccurate.

(3) If—

(a) a UK competent authority incorrectly transmits personal data to a non-UK competent authority; and

(b) the latter authority is required, in accordance with the Data Protection Framework Decision, to pay compensation to the data subject for damage caused by use of the incorrectly transmitted data,

the former must pay to the latter, on request and the provision of satisfactory evidence, an amount not exceeding the sum awarded in respect of that damage.

Confidentiality of processing

46.—(1) A person who has access to personal data in connection with activities referred to in regulation 29 may process that data only if that person is a member of, or acts on instructions of, a UK competent authority, unless he is required to do so by an enactment or rule of law.

(2) A person working for a UK competent authority may only process such personal data in accordance with this Part.

Security of processing

47.—(1) A UK competent authority must implement appropriate technical and organisational measures to protect personal data against—

(a) accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves transmission of that data over a network or making it available by granting direct automated access; and

(b) all other unlawful forms of processing.

(2) In doing so, that authority must take into account, in particular, the risks represented by the processing and the nature of the data to be protected.

(3) Such measures must ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of their implementation.

(4) A UK competent authority must in respect of automated data processing adopt measures, policies and practices designed to—

(a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);

(b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(d) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment (communication control);

(g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity).

(5) Where a UK competent authority wishes to designate a data processor to carry out processing on its behalf, the authority—

(a) may do so only if the processor guarantees that it will—

(i) observe the requisite technical and organisational measures required by virtue of paragraph (1); and

(ii) comply with instructions given by that competent authority; and

(b) must monitor the processor in those respects.

(6) Personal data may be processed by a processor only on the basis of a legal act or a written contract.

Prior consultation

48.—(1) A UK competent authority that wishes to process personal data in the circumstances described in paragraph (2) must consult the Commissioner before doing so.

(2) Those circumstances are that the processing of the data will form part of a new filing system to be created where—

(a) sensitive personal data are to be processed; or

(b) the type of processing, in particular using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.