WQ.387/2019

WRITTEN QUESTION TO H.M. ATTORNEY GENERAL
BY DEPUTY M.R. HIGGINS OF ST. HELIER
ANSWER TO BE TABLED ON TUESDAY 24th SEPTEMBER 2019

Question

Further to his answer to Oral Question 214/2019, will H.M. Attorney General explain how a telephone intercept is considered lawful and not in breach of the Data Protection (Jersey) Law 2018 in instances where the warrant authorizing the intercept is for one specific number or person but, in error, the police intercept the communications of another person not connected with the warrant or the subject of the investigation?

Answer

A telephone intercept is considered lawful for the purposes of the Data Protection (Jersey) Law 2018 (the 'Law') because the warrant authorising the intercept is for a 'law enforcement purpose'. For the purposes of the Law both the Law Officers' Department and the States of Jersey Police are a 'competent authority'. When a 'competent authority' processes personal data for a 'law enforcement' purpose as defined in Article 1(1) of the Law the provisions of Schedule 1 to the Law apply.

Schedule 1 modifies Article 8(1)(a) of the Law to the extent that the personal data does not need to be processed transparently, but all the principles in Article 8 apply, including the need to process the personal data lawfully and fairly (Article 8(1)(a)).

'Lawfulness' as defined in Article 9 is modified by Schedule 1 to the extent that if the processing of personal data is for a 'law enforcement purpose', such processing will be lawful.[1]

Therefore, where a warrant authorising the intercept for a specific telephone number is the subject of approval granted by the Attorney General, then it is lawful for the purposes of the Data Protection Law.

The Code of Practice on interception of communications made under the Regulation of Investigatory Powers (Jersey) Law 2005 ('RIPL') provides that obtaining a warrant will only ensure that the interception authorized is a justifiable interference with an individual's rights under Article 8 of the European Convention of Human Rights (the right to privacy) if it is necessary and proportionate for the interception to take place. RIPL recognises this by first requiring that the Attorney General believes that the authorization is necessary on one or more of the statutory grounds set out in Article 10(3) of RIPL. If the interception is necessary, the Attorney General must also believe that it is proportionate to what is sought to be achieved by carrying it out. This involves balancing the intrusiveness of the interference, against the need for it in operational terms.

All material (including related communications data) intercepted under the authority of a warrant must be handled in accordance with safeguards imposed upon the Attorney General by RIPL. Article 19 of RIPL requires that disclosure, copying and retention of intercept material be limited to the minimum necessary for the authorized purposes. Any breach of these safeguards must be reported to the Investigatory Powers Commissioner.

A 'personal data breach' under the Data Protection Law can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the

[1] Subject to Article 9(2) – (4) of Schedule 1 being met in the event any special category data is processed. The modified Article 9 does not require a processing condition in Schedule 2 to apply.

data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

If it becomes clear that despite a warrant authorising the intercept for a specific telephone number, which is the subject of approval granted by the Attorney General, the telephone number of a person not connected with the subject of the investigation is intercepted, the interception is immediately terminated in accordance with the safeguards imposed by RIPL. Access to personal data has occurred with proper authorisation and a data protection breach has not occurred.

However where, in error, the police intercept the wrong phone number (i.e. not one authorised by the warrant) the police would again conclude the call as soon as the error is identified in accordance with the safeguards imposed by RIPL. The warrant authorizing the intercept of the correct number is still based on lawful authority. But to intercept the wrong number would be a personal data breach.

In both scenarios the Investigatory Powers Commissioner would be informed. Only in the case of when a personal data breach is likely to result in a risk to the rights and freedoms of natural persons must a personal data breach be reported to the Data Protection Authority.