An Bille um Shonraí Clárúcháin Feithicle (Cuardach agus Malartú Uathoibrithe), 2018
Vehicle Registration Data (Automated Searching and Exchange) Bill 2018

Meabhrán Mínitheach agus Airgeadais
Explanatory and Financial Memorandum

AN BILLE UM SHONRAÍ CLÁRÚCHÁIN FEITHICLE (CUARDACH AGUS MALARTÚ UATHOIBRITHE), 2018

VEHICLE REGISTRATION DATA (AUTOMATED SEARCHING AND EXCHANGE) BILL 2018

EXPLANATORY AND FINANCIAL MEMORANDUM

Purpose of the Bill

The purpose of this Bill is to give effect to certain measures of the European Council Decisions 2008/615/JHA and 2008/616/JHA (generally referred to as the 'Prüm Decisions' after the town in Germany where the basis of the Decisions was originally agreed); and to provide for related matters. The Decisions are binding on all EU Member States who choose to opt into them. Ireland chose to opt in by votes in both Houses of the Oireachtas.

The Prüm Decisions are aimed at stepping up cross-border cooperation, particularly in combating terrorism and cross-border crime, and provide in particular for the automated exchange of DNA, Fingerprint (dactyloscopic) and Vehicle Registration Data (VRD). Legislation in relation to sharing of DNA and fingerprint data is the responsibility of the Department of Justice and Equality, and that legislation is in place.

The Department of Transport, Tourism and Sport (DTTAS) has responsibility for the aspects of the Decisions relating to VRD. The present Bill is intended to provide the necessary legislative basis for the introduction of sharing of VRD in accordance with the Decisions.

Financial Implications – The Bill will not have any financial impact for the Exchequer.

Section 1 – Interpretation

This is a standard provision.

Section 2 – National contact point in State - vehicle registration data

The Prüm Decisions require each EU Member State to designate a national contact point for exchange of VRD under the Decisions. The Minister for Transport, Tourism and Sport is designated by *section 2* as the national contact point in the State, on the grounds that the Minister is the statutory holder of the data concerned.

Section 3 – Automated searching of vehicle registration data held in National Vehicle and Driver File

Section 3 provides for national contact points of other Member States, as well as Iceland and Norway, to conduct searches of vehicle registration data in accordance with the Decisions. The inclusion of Iceland and Norway reflects an agreement between the EU and these jurisdictions.

Section 3(1) allows access to Irish VRD for national contact points of the states concerned and specifies the purposes for which they may access the data. The Decisions require that searches may be conducted only with a full Vehicle Identification Number (VIN) or full registration number, and this is set out in *section 3(2)*. *Section 3(3)* details the contents of a reply to such a search, both in cases where a response is found and in cases where one is not. Under *section 3(4)*, any data provided by the national contact point of another state conducting a search of NVDF data may be used only for the purposes of that search and of maintaining records (in accordance with section 6 below) of searches. *Section 3(5)* provides for the deletion of data received from a searching member state, subject to the maintenance of records under section 6.

Section 4 – Automated searching of vehicle registration data held by designated states

This section provides for searches of VRD held by other Member States, Iceland or Norway, to be conducted by the national contact point in the State pursuant to the Decisions.

Section 4(1) allows the national contact point in the State to conduct searches of VRD held by other EU Member States, or Iceland and Norway, in accordance with the Decisions. *Section 4(2)* requires that it should be the national contact point in the State which receives a response to such a request. Under *section 4(3)*, searches may be conducted only with a full Vehicle Identification Number (VIN) or full registration number (see section 3(2) above for incoming search requests). *Section 4(4)* stipulates that data received from another state by the national contact point of the State may be used only for the purposes for which it was provided, unless the national contact point of the state which provided the data permits otherwise. *Section 4(5)* allows the national contact point in the state to share data received – with the prior authorisation of the national contact point of the state which provided the data – with the Courts, the Garda Síochána, the Director of Public Prosecutions, or others deemed appropriate.

Section 5 – Correction of inaccurate data and deletion of incorrectly supplied data

This section provides for the correction of inaccurate data and for circumstances where data are received which should not have been.

Section 5(1) places an obligation on the national contact point in the State, in cases where it comes to its attention that data sent by it to the national contact point of another state are incorrect or should not have been supplied, to contact that other national contact point and ask them to amend or delete the data, as appropriate. Under *section 5(2)*, when the national contact point receives data unrequested from the national contact point of another state, it shall immediately check whether the data are necessary for the purposes for which they were supplied. The correction or deletion of erroneous data received by the national contact point in the State is addressed by *section 5(3)*.

In addition, section 5 requires: the deletion of data received by the national contact point when they are no longer required (*5(4)*); the national contact point to inform a data subject where the data subject has contested the accuracy of the data related to them and that accuracy cannot be established (*5(5)*); following of procedures for marking data as being of undetermined accuracy and circumstances for removing such mark (*5(6)*); the national contact point in the State to delete data which should not have been supplied to it by another national contact point (*5(7)*). The national contact point may also block rather than delete data where deletion might prejudice the interests of the data subject – further processing of blocked

data is limited to purposes related to the interests of the data subject (*5(8)-(9)*).

Section 6 – Recording of automated supply of personal data

In accordance with the requirements of the Decisions, procedures must be set out for the recording of supply of data under the Decisions.

Section 6(1) requires the national contact point in the State to maintain records of data exchange under the Decisions. The details to be recorded are set out in *6(2)*. *6(3)* limits the use of such records to monitoring data protection and security. Under *6(4)*, these records are to be maintained for 2 years and then deleted. The national contact point is required to make these records available on request to the Data Protection Commissioner (DPC) (*6(5)*), and to conduct checks of its own on the records to monitor lawfulness of supply and receipt of data, the results of which are to be retained for 18 months and made available on request to the DPC (*6(6)*).

Section 7 – Data Protection Commissioner's functions

The Data Protection Commissioner (DPC), has a number of functions in relation to the Decisions, which provide specific requirements for data protection. It is important to note that a new EU framework of data protection law, based on the General Data Protection Regulation (GDPR) and the Policing Directive, is due to come into effect from May 2018. However, the Policing Directive, which would otherwise be the new instrument applicable to the Prüm Decisions, explicitly states that it does not apply to Prüm, and that the data protection measures prior to the Policing Directive and the GDPR will continue to apply to the Prüm Decisions. This means that, while Irish data protection legislation is currently being updated to meet the requirements of the GDPR and the Policing Directive, the current legislation based on the Data Protection Act 1988 will continue to apply in the case of the Prüm Decisions.

Section 7(1) and *7(10)* establish the responsibility of the DPC in relation to data protection and the exchange of information under the Decisions. The DPC is to monitor the lawfulness of data processing under this legislation (*7(2)*), carry out random checks on data processing under the legislation (*7(3)*), and examine the lawfulness of processing of data related to individual data subjects on request from such data subjects (*7(4)*). The results of checks under *7(3)* or (4) are to be retained for 18 months (*7(5)*). Given the international aspect of the data sharing, section *7(6)-(9)* sets out circumstances in which the DPC may or shall liaise with data protection authorities in another state with which or by which data are shared under the Decisions.

Section 8 – Application of Data Protection Act 1988

Section 8 applies current data protection law as enshrined in the Data Protection Act 1988 to the operation of processing of information under the Decisions. As set out above (under section 7), this legislative framework will continue to apply after the introduction of new EU data protection rules for other circumstances from May 2018.

Section 9 – Duties of data controllers

Section 9(1) requires data controllers to comply with the technical requirements of the Decisions, as well as requiring them to ensure the appropriate level of data security. A data controller may not use inaccuracy of data as grounds for avoiding liability (*9(2)*). *Section 9(3)* allows the Minister, as the national contact point in the State, in a case where the Minister has incurred damages due to the inaccuracy of data received from a national contact point in another State, to seek to recoup the damages from the other national contact point. Similarly, *section 9(4)* requires

the Minister to refund any damages paid by the national contact point of another state arising from the inaccuracy of data supplied by the Minister under the Decisions.

Section 10 – Authorised officers

Under the Prüm Decisions, the persons processing data in accordance with the Decisions must be 'authorised officers.' *Section 10(1)* permits the Minister to appoint authorised officers from among members of An Garda Síochána or officials of the Minister, and to revoke such appointments (*10(2)*). The Minister is required to provide on request details of authorised officers to the Data Protection Commissioner, the national contact point of another State, or the data protection authority of another State. *Section 10(4)* provides that only authorised officers may conduct automated searches for the purposes of the Decisions.

Section 11 – Short title and commencement

This is a standard provision.

An Roinn Iompair, Turasóireachta agus Spóirt,
Eanáir, 2018.

Wt. —. 330. 1/18. Essentra. (70178). Gr. 30-15.