Ministry of JUSTICE

Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals

January 2013

Government response to Justice Select Committee's opinion on the European Union Data Protection framework proposals

Presented to Parliament
by the Lord Chancellor and Secretary of State for Justice
by Command of Her Majesty

January 2013

Cm 8530 £6.25

Any enquiries regarding this publication should be sent to us at: nicola.calderhead@justice.gsi.gov.uk or 020 3334 5408.

This publication is available for download at www.official-documents.gov.uk and on our website at www.justice.gov.uk

ISBN: 9780101853026

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 2533713 01/13

Printed on paper containing 75% recycled fibre content minimum.

Contents

The approach to reforming the current data protection framework

We are concerned that the approach taken by the European Commission, introducing two instruments, will lead to a division of the UK law, set out in the Data Protection Act. We believe that this could cause confusion, both for data subjects, and for organisations within the criminal justice system in particular, as they will have to consider which law applies in their given circumstance. We are also concerned that this twin-track approach might also lead to inconsistencies in application, both due to differing provisions in the instruments and over time, due to court decisions under each instrument. If this is still to be the approach, we recommend that there is consistency between the two instruments from the outset, to mitigate the future divergence in their application. Furthermore, the UK Government and the Information Commissioner's Office will be required to work effectively together in order to produce and disseminate effective guidance so that data subjects know their rights and organisations know their responsibilities under each law. (Paragraph 13)

The UK Government's position with regard to the proposed Regulation is that it should be re-cast as a Directive. With regard to the proposed Directive covering processing in the area of police and judicial co-operation, the Government does not believe that the case for replacing and repealing the Framework Decision 2008/977/JHA has been convincingly made.

If the proposed Regulation were to be changed to a Directive and the proposal for a Directive were to be taken forward, then there would be two Directives, one for the general data protection framework and one for processing in the area of police and judicial co-operation in criminal matters. An advantage of this approach would be that the two Directives could then be implemented in a single piece of domestic legislation to help avoid confusion and support consistency where necessary.

With regard to the Committee's call for consistency between the two instruments, the Government believes that, as far as it is possible, there should be parallels between the two instruments. It is however important that the different contexts in which the instruments have been proposed are considered: the draft Regulation has been proposed for general data processing, whereas the draft Directive applies in the field of police and judicial co-operation in criminal matters. The use of data in the areas covered by each instrument is very different and there is a need for greater flexibility in the field of police and judicial co-operation due to the operational requirements in this area and, where necessary, this should be reflected in the two instruments. Recital 10 of the draft Directive refers to Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal

matters and police co-operation,[1] which acknowledged that specific rules may be needed for the protection of personal data in this field.

The Government notes the Committee's call for it to work with the ICO to disseminate effective guidance. We would expect the ICO to provide relevant guidance following the adoption of the instruments.

[1] Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Lisbon Treaty.

The draft Regulation

Arguments for and against a Regulation

Bringing EU data protection legislation up-to-date is necessary and could provide benefits to both individuals and businesses. Many of these benefits are only attainable if there is effective harmonisation of laws across Member States, and therefore we can understand why the European Commission decided that a Regulation was the correct instrument to achieve their objective. However, by setting out prescriptive rules there is no flexibility to adjust to individual circumstances. We believe that the Regulation should focus on stipulating those elements that it is essential to harmonise to achieve the Commission's objective, such as the consistency mechanism and the establishment of the European Data Protection Board. Member States' data protection authorities should be entrusted to handle factors associated with compliance, such as the level of fees or when it should be informed about a data protection impact assessment, whilst also being a source of guidance. Consistency of approach should then be delegated to the European Data Protection Board. (Paragraph 30)

The Government's position that the proposed Regulation should be re-cast as a Directive would allow for harmonisation in the areas where it is advantageous and flexibility for Member States where it is required. The European Commission's Impact Assessment acknowledges that harmonisation could be achieved through the use of a Directive.[2]

For example there could be harmonisation of: the fundamental principles found within the proposals; the rights that data subjects enjoy; and the rules relating to independent supervisory authorities and the European Data Protection Board. The Government also supports the principle of the consistency mechanism. We believe that the data protection framework should protect the civil liberties of individuals. This means putting rules in place that ensure that the processing of personal data is fair, secure, and that data should be retained for no longer than is necessary.

EU data protection legislation must secure individuals' privacy without placing constraints on businesses practices that harm innovation and growth. For

---

[2] European Commission, Working Document. Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Pg 46

example, the proposed Regulation places prescriptive obligations upon data controllers as to how they will comply with the proposed Regulation, such as completing data protection impact assessments and hiring data protection officers. This is a 'one size fits all' approach which does not allow data controllers (from small online retailers to multinational Internet companies) to adopt their own practices in order to ensure compliance with the legislation. The European Commission's proposal should focus on regulating outcomes, not processes.

Impact assessment

We call on the European Commission to work with the UK Government, the governments of other Member States, and other stakeholders, and to pool resources, expertise and information, so that a full assessment of the impact of the proposals can be produced. (Paragraph 37)

The Government published its own Impact Assessment on the proposals on Thursday 22 November 2012. While the assessment focused on the impact of the proposals on the UK economy, it also provided an assessment of the Commission's Impact Assessment, including an explanation as to why the Government believes the administrative saving of €2.3 billion per annum estimated by the Commission is a significant over-estimate.

The Government's Impact Assessment recognises that while there are benefits from the proposed Regulation, such as a reduction in legal fragmentation, these benefits are outweighed by the costs of additional administrative and compliance measures that the draft Regulation introduces. The Impact Assessment concludes that the proposed Regulation in its current form could have a net cost to the UK economy of £100–£360 million per annum (in 2012–13 earnings terms). The Government is seriously concerned about the potential economic impact of the proposed Regulation. At a time when the Eurozone appears to be slipping back into recession, reducing the regulatory burden to secure growth must be the priority for all Member States. It is therefore difficult to justify the extra red-tape and tick box compliance that the proposal represents. For example, we estimate the costs for UK small businesses of simply demonstrating compliance with the proposals to be around £10 million (in 2012–13 earnings terms) every year.

We have shared the Government's Impact Assessment with the European Commission, EU Member States, and other stakeholders. We would encourage interested parties to use the Government's Impact Assessment in their own analysis and the Ministry of Justice would welcome any feedback.

Impact on the Information Commissioner's Office

We regard as authoritative the UK Information Commissioner's assertion that the system set out in this draft Regulation "cannot work" and is "a regime which no-one will pay for", and we believe that the Commission needs to go back to the drawing board and devise a regime which is much less prescriptive, particularly in the processes and procedures it specifies. (Paragraph 43)

The Government agrees with the ICO's assertion that the system set out in the draft Regulation 'cannot work' and is 'a regime which no-one will pay for'. Under the risk-based model that the UK is advocating, it would be for data controllers to put measures in place in order to comply with the outcomes prescribed in the legislation.

The ICO has estimated that the additional requirements outlined in the proposed Regulation could cost it between £8–£28 million per annum not accounting for the loss of the notification fee income. These additional costs have been factored into the UK's Impact Assessment on the proposals.

General comments on the draft Regulation

We note that both the Government and the Information Commissioner believe that the necessary changes in the Regulation and the Directive can be agreed through negotiation, and we support them in their efforts to achieve this. (Paragraph 55)

We welcome the Committee's ongoing support for the Government as we negotiate on making the necessary changes to the two instruments.

The "right to be forgotten"

The right of citizens to secure the erasure of data about them which is wrongly or inappropriately held is very important, but it is misleading to refer to this as a "right to be forgotten", and the use of such terminology could create unrealistic expectations, for example in relation to search engines and social media. (Paragraph 63)

The Government is in favour of appropriate deletion rights for data subjects. However we share the Committee's concerns surrounding the "right to be forgotten". We question the practicality of Article 17(2) of the proposed Regulation which places obligations on data controllers to inform third parties of the data subject's request for deletion. This would be extremely difficult, if not impossible, to achieve when information has been posted on the Internet. We therefore consider that this article raises unrealistic expectations for consumers that their data can be deleted when it has been passed on to third parties. This may encourage data subjects to be more reckless with their personal data, thus undermining the intention of enhancing their protection and rights.

Subject access rights

An individual's right of access to their own personal data is a fundamental right; and individuals should not be required to pay a fee to make a subject access request. We urge the Government to change its negotiating position to one which accepts that subject access rights should be exercisable free of charge. (Paragraph 77)

The UK supports the principle that data subjects should have access to their personal data, but burdens on data controllers must be proportionate. Responses that we received to our Call for Evidence expressed a real concern that the removal of a fee will lead to an influx of repeated and vexatious requests for personal data. The Government's Impact Assessment showed that the number of requests could increase by 25–40 per cent, leading to additional costs of £12–£37 million per annum (in 2012–13 earnings terms) for the 4,600 businesses already receiving large numbers of requests. We would therefore be in favour of retaining the flexibility in the current framework and for data controllers to be able to charge a small fee for subject access requests and we note that not all data controllers currently charge a fee.

Furthermore, the Government considers that charging a fee is compatible with fundamental rights. In this context, the legitimate aim behind charging the fee is to dissuade abuse of the system which would put a disproportionate burden on data controllers. The fee which data controllers may presently charge under UK law is proportionate. It is nominal, and there is no obligation on the data controller to charge the fee.

Obligation to appoint Data Protection Officers

We believe that if the requirement to employ a Data Protection Officer is retained it should be based on the type of business and the sensitivity of data that is handled, rather than the number of employees. (Paragraph 81)

The Government does not believe that the requirement to have a data protection officer (DPO) is necessary in the proposed Regulation and we believe that there are other means of achieving the accountability principle. As the proposal stands, an SME processing personal data may be unsure of whether it falls within the category of controllers which are required to designate a data protection officer, whilst a larger enterprise would be required to hire a DPO even though it may not be necessary. It is envisaged that DPOs are expected to be one of the most costly elements of the Regulation for micro entities and SMEs that carry out 'regular and systematic processing' of personal data. The Government's Impact Assessment estimates that there could be around 42,000 micros and SMEs needing to employ a DPO, costing anywhere between £30–£180 million per annum (in 2012–13 earnings terms) depending on the contractual hours of the DPO.

Under the risk based model that the UK Government is proposing, data controllers would be encouraged to appoint data protection officers if they were felt necessary to ensure compliance with the proposed Regulation.

Whether or not a DPO is appointed could depend on the quantity and the sensitivity of the data that is being handled.

Sanctions

We believe that data protection authorities should have more discretion as to the sanctions that they can impose in order to effectively punish the worst behaviour. We are aware that this could result in different approaches being taken in each Member States, and therefore recommend that, where there is evidence that such differences are having a deleterious effect on compliance, the European Data Protection Board be entrusted to provide guidelines on the type of sanction that may be appropriate in given situations. (Paragraph 87)

The Government believes that the supervisory authorities should have more discretion in the imposition of fines and that the proposed removal of discretion, combined with the higher levels of fines, could create an overly risk-averse environment for data controllers. Were there to be divergence in terms of the use or the levels of fines, and if those differences had a negative effect on compliance, the Government considers that the provision of guidelines by the European Data Protection Board could be useful.

Excessively high fines can be detrimental to economic growth since they may lead to over-spending on compliance, may discourage new start-ups in industries where processing of personal data is central to the business, and can lead to insolvency. While an effective fine must be high enough to incentivise compliance, it should not be so high that it creates an unnecessary level of risk adversity amongst data controllers.

Concerns raised by specific groups

The Government have told us that some organisations who submitted written evidence to us have not shared their concerns with them. We call on the Government to consider the points raised in paragraphs 90 to 100, and in more detail in written evidence, and inform us as to how, where necessary, they will be addressed in negotiations. (Paragraph 101)

The Government has met representatives from all of the sectors that the Committee outlined in this section and representatives from the respective sectors all attended a Data Protection Advisory Panel that the Ministry of Justice held.

With regard to the specific issues that the committee raises from these sectors, the Government agrees that there is a need to ensure that the Regulation does not hinder processing, such as that undertaken by credit reference agencies, from taking place.

However, with regard to Equifax's suggestion that the proposals overlooked an important distinction between 'citizen data' and 'consumer data', the Government is in agreement with the ICO when it stated that a sensible,

proportionate system was required, regardless of whether it is 'citizen data' or 'consumer data' being used.

The Brussels European Employee Relation Group stated that the proposed Regulation was overly centred on issues relating to social media business. As Lord McNally explained in his evidence session, the Government is aware of this concern and we are working to provide a sensible, coherent set of rules that can apply to all data controllers.

The Newspaper Society raised concerns about how the right to be forgotten would comply with Article 80 and the processing of personal data and freedom of expression. As Lord McNally outlined in his evidence to the Committee, Article 80 outlines that EU Member States can provide for exemptions or derogations from the provisions found in Chapter III, including Article 17 and the right to be forgotten.

The BMA raised concerns surrounding Article 83 and the Ministry of Justice responded that we are aware that the individual citizen is very concerned that their medical records are not able to be disseminated in an improper way. The Government will negotiate to ensure that the Regulation provides robust data protection for individuals, whilst ensuring that obligations on researchers are workable and proportionate.

In response to the concerns expressed by the Association of British Insurers, the Government recognises the importance of fraud prevention and is working to ensure that the proposals are sufficiently flexible to enable processing for the purposes of prevention fraud to take place.

The Committee's opinion – Regulation

The Regulation is necessary, first to update the 1995 Directive and take into account past and future technological change; and secondly to confer on individuals' rights that are necessary to protect their data and privacy as stipulated in the Lisbon Treaty and the EU Charter of Fundamental Rights. (Paragraph 102)

The majority of respondents to the Government's Call for Evidence welcomed the proposed update of EU data protection legislation, particularly in relation to the strengthening of the single market. The Government recognises that the uses of data have changed since the current Directive was agreed in 1995 and that the current framework therefore needs updating.

The proposed Regulation, in keeping with the aims of the 1995 Directive, is intended to protect individuals with regard to the processing of their personal data. The protection of personal data is an aspect of the right to respect for private and family life under Article 8 of the ECHR.[3] Article 8 of the ECHR, as re-stated in Article 7 of the Charter of Fundamental Rights of the EU, guarantees the right to respect for private and family life. Article 8 of the Charter re-states the specific right to the protection of personal data.

Article 16(2) of the Treaty on the Functioning of the European Union is the new legal base for data protection legislation, introduced by the Lisbon Treaty. Article 16 empowers the European Parliament and the Council to lay down rules on the protection of individuals with regards to the processing of personal data. However, the Government does not consider that the introduction of the new legal base requires the Commission to propose legislation where there is no compelling case to do so and the Government considers that there is no need to replace the Framework Decision at this time.

The Government wants to see EU data protection legislation which protects the civil liberties of the individual whilst allowing for proper public protection and economic growth and innovation. These should be achieved in tandem, not at the expense of one or the other.

[3] Recitals 10 and 11 of the 1995 Directive refer to Article 8 of the ECHR and the right to privacy.

However, the Regulation as drafted is over-prescriptive as to how businesses and public authorities should comply to ensure these rights are upheld. We have been told that the Information Commissioner's Office will require substantial extra resources, and businesses have argued that many administrative burdens will be imposed on them. (Paragraph 103)

The Government agrees with the Committee's view that the proposed Regulation as drafted is over-prescriptive in terms of how data controllers comply with the draft Regulation. Under the risk-based model that the UK is advocating, it would be for data controllers to put in place and regulate the obligations in order to ensure compliance with the legislation.

The Government is sympathetic to the Information Commissioner's assertions that the proposals as they stand are, 'a regime which no-one will pay for'. The UK's Impact Assessment accounted for the additional resource need estimated by the ICO of £8–£28 million per annum, and also assessed the cost to the ICO of the loss of its notification fee income.

We believe that the European Commission has a choice: It can continue to pursue the objective of harmonisation through a Regulation by focusing on the elements that are essential to achieve consistency and cooperation across Member States, whilst entrusting the details on compliance to the discretion of data protection authorities and the European Data Protection Board; alternatively, it can use a Directive to set out what it wants to achieve in all the areas contained in the draft Regulation, but then leave implementation in the hands of Member States, and forgoing an element of harmonisation and consistency. (Paragraph 104)

The Government's position that the proposed Regulation should be re-cast as a Directive would allow for harmonisation in the areas where it is advantageous and flexibility for Member States where it is required. The European Commission's Impact Assessment acknowledges that harmonisation could be achieved through the use of a Directive.[4]

For example there could be harmonisation of: the fundamental principles found within the proposals; the rights that data subjects enjoy; and the rules relating to independent supervisory authorities and the European Data Protection Board. The Government also supports the principle of the consistency mechanism. We believe that the data protection framework

---

[4] European Commission, Working Document. Impact Assessment: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Pg 46

should protect the civil liberties of individuals. This means putting rules in place that ensure that the processing of personal data is fair, secure, and that data should be retained for no longer than is necessary.

EU data protection legislation must secure individuals' privacy without placing constraints on businesses practices that harm innovation and growth. For example, the proposed Regulation places prescriptive obligations upon data controllers as to how they will comply with the proposed Regulation, such as completing data protection impact assessments and hiring data protection officers. This is a 'one size fits all' approach which does not allow data controllers (from small online retailers to multinational Internet companies) to adopt their own practices in order to ensure compliance with the legislation. The European Commission's proposal should focus on regulating outcomes, not processes.

To answer the European Scrutiny Committee's specific question to us: As currently drafted, the Regulation does give data subjects essential rights that must not be compromised during negotiations, and it has the potential to make data protection compliance easier for businesses, especially small businesses, which trade across the European Union. However, we do not believe that in its present form it will produce a proportionate, practicable, affordable or effective system of data protection in the EU. (Paragraph 105)

The Government notes the Committee's response to the European Scrutiny Committee. The Government wants to see data protection law which protects the civil liberties of individuals. We want to achieve protection for individuals whilst ensuring that data controllers can process data without having to comply with expensive and bureaucratic measures which do not enhance data protection and which prevent businesses from growing.

The draft Directive

We are not convinced that there is a pressing need to alter EU law in this area, given that the Framework Decision 2008 was only recently implemented. However, it is arguable that since the general 1995 Directive requires updating, the corresponding legislation which deals with criminal matters should also be updated so that the principles in each instrument are consistent. (Paragraph 114)

The Government shares the Committee's view that there is not a pressing need to update the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The Framework Decision has yet to be fully implemented across all Member States, or evaluated. Implementation and evaluation of the current legislation should come first before new legislation is considered.

We agree with the Information Commissioner that data protection principles should be consistent across both the draft Regulation and the draft Directive. We recommend that during the negotiations on the legislation, the Government seek to amend the draft Directive so that this consistency is achieved. (Paragraph 121)

With regard to the Committee's call for consistency between the two instruments, the Government believes that, as far as it is possible, there should be parallels between the two instruments. It is however important that the different contexts in which the instruments have been proposed are considered: the draft Regulation has been proposed for general data processing, whereas the draft Directive applies in the field of police and judicial co-operation in criminal matters. The use of data in the areas covered by each instrument is very different and there is a need for greater flexibility in the field of police and judicial co-operation due to the operational requirements in this area and, where necessary, this should be reflected in the two instruments. Recital 10 of the draft Directive refers to Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation,[5] which acknowledged that specific rules may be needed for the protection of personal data in this field.

[5] Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Lisbon Treaty.

It needs to be clear beyond doubt that exchange of information between UK law enforcement agencies is not covered by the Directive, and the Government's negotiating stance should seek to ensure that the exemption of the UK from provisions relating to domestic processing is written into the Directive. In order to clarify the position, the Ministry of Justice should provide an impact assessment of the draft Directive on the basis that domestic processing does not apply to the UK. (Paragraph 128)

As detailed further below in response to paragraph 143, the Government believes that the inclusion of domestic processing in the draft Directive is at odds with the principle of subsidiarity. Under this principle, the form of Community action should be as simple as possible, and leave as much scope as possible for national decision. Furthermore, there is no evidence to demonstrate that the lack of EU rules in this area has had a detrimental impact on law enforcement activity or the protection of individuals. It is our view that introducing prescriptive requirements for domestic processing may instead have a detrimental effect on law enforcement operations, placing onerous burdens on data controllers and huge costs on public authorities – without delivering better data protection for individuals. The Government therefore does not consider that full harmonisation of police and judicial co-operation in criminal matters is necessary or desirable. Any instrument in this area should therefore set a minimum standard and allow member states the flexibility to adopt higher standards where that is considered appropriate.

A core negotiating aim, therefore, is to press for the removal of the application of the Directive to domestic processing. The Government's view of the effect of Article 6a of the opt-in protocol[6] is that any provisions on domestic processing in the Directive will only apply to the UK (and Ireland) where data is being processed for the purposes of an EU instrument in which the UK participates. The domestic processing provisions would, therefore, not apply where data processing was wholly for domestic purposes, such as between a police force and a prison.

It is worth noting that organisations which process criminal justice data will also process personal data covered under the Regulation and so some of the monetised costs and benefits stemming from the Regulation could be shared (for example, the cost of designating a data protection officer). There is a degree of flexibility for Member States in determining how the EU-level rules in the proposed Directive would be implemented and a fuller assessment of the costs and benefits specific to the proposed Directive will be produced nearer the point of implementation.

---

[6] Article 6a is a specific provision on data protection that means that were measures under Article 16 concern policing and criminal justice they only apply to the UK to the extent that they relate to processing done under EU measures on police and criminal justice which the UK has signed up to.

We understand that the Directive does not apply to domestic processing by law enforcement agencies within the UK, and it should be placed beyond doubt that this is the case. We have noted the evidence of the Association of Chief Police Officers, that the Directive might nevertheless impact on the ability of the police to use common law powers to pass on information in the interests of crime prevention and public protection, and we believe that it needs to be made clear beyond doubt that it must not have this effect. We also agree with ACPO that the Directive, like the Regulation, is unnecessarily prescriptive about the structures and processes for securing data protection compliance. (Paragraph 133)

As noted in response to paragraph 128, the Government is negotiating to secure language in the Directive to reflect its application to the UK. Similarly, on the issue of common law, the Government shares the view of ACPO and the Committee that the Directive should not undermine the use of common law powers in the UK or other countries with similar systems.

The Government argues that the current lack of EU legislation on domestic processing has not obstructed cooperation between Member States, but the European Commission argues that it does cause difficulties for a number of Member States. We call on the Government to explain further why they are opposed to domestic processing for other Member States, given the current position that it will not apply to the UK, and to clarify what impact the changes would have on cooperation with the UK. (Paragraph 143)

The Government is opposed to the inclusion of domestic processing in the proposed Directive based on the principle of subsidiarity. For European Union action to satisfy the principle of subsidiarity, it is necessary to show both that the objectives of the proposed action cannot be sufficiently achieved by the Member States acting on their own, and that they can therefore be better achieved by action on the part of the Union. The Government is not convinced that the provisions of domestic processing comply with the principle of subsidiarity. Domestic processing is by its nature internal to a Member State and we have not been presented with any evidence to suggest that the changes would have an impact on cooperation with the UK.

The Committee's opinion – Directive

From the point of view of the data subject, the draft Directive provides a weaker level of data protection in comparison to the draft Regulation. We recognise the significant differences in the handling of sensitive personal data by law enforcement authorities, but in a number of respects this lower level of protection does not appear justifiable. During negotiations, the Government should seek to amend the draft Directive so that data protection principles are as consistent as possible across both EU instruments. This will additionally ensure that the rights set out in the Lisbon Treaty are upheld. (Paragraph 149)

As set out above, with regard to the Committee's call for consistency between the two instruments, the Government believes that, as far as it is possible, there should be parallels between the two instruments. It is however important that the different contexts in which the instruments have been proposed are considered: the draft Regulation has been proposed for general data processing, whereas the draft Directive applies in the field of police and judicial co-operation in criminal matters. The use of data in the areas covered by each instrument is very different and there is a need for greater flexibility in the field of police and judicial co-operation due to the operational requirements in this area and, where necessary, this should be reflected in the two instruments. Recital 10 of the draft Directive refers to Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation,[7] which acknowledged that specific rules may be needed for the protection of personal data in this field.

In terms of the level of protection provided by the Directive, as opposed to the draft Regulation, there is no contradiction between providing a more flexible instrument and the delivery of fundamental rights. The Framework Decision, for example, is a minimum standards instrument. Recital 48 of the Framework Decision confirms that it respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights.

[7] Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, annexed to the final act of the intergovernmental conference which adopted the Lisbon Treaty.

The Government's position is that the Directive will have limited application to the UK, due to Article 6a of Protocol 21 of the Treaty on the Functioning of the European Union. If this is the case, we believe it will be beneficial to the UK as law enforcement authorities will not be bound by over-prescriptive measures contained within the Directive. This would also mean that EU law will not apply to the domestic processing of data, such as between police forces. Domestic processing for criminal justice matters will continue to be covered by the Data Protection Act 1998. (Paragraph 150)

The Government's position is that the proposed Directive will not apply to the processing of data outside of an EU instrument. Where the draft Directive does not apply, domestic law will continue to govern the processing of such personal data.

To answer the European Scrutiny Committee's specific question to us: As currently drafted, the Directive does not sufficiently protect personal data. In particular, the level of data protection is not to the same standard as that contained in the draft Regulation which covers general data protection matters. We are concerned that it should be clear that domestic processing of data within the UK by law enforcement agencies will not be covered or restricted by the Directive, and it should also be clear that Member States have the flexibility to implement the Directive in ways which achieve its purposes through processes which are appropriate and proportionate in the national context. (Paragraph 151)

In terms of the level of protection provided by the Directive, as opposed to the draft Regulation, there is no contradiction between providing more flexible instrument and the delivery of fundamental rights. The Framework Decision, for example, is a minimum standards instrument. Recital 48 of the Framework Decision confirms that it respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights.

As set out above, with regard to the Committee's call for consistency between the two instruments, the Government believes that, as far as it is possible, there should be parallels between the two instruments. It is however important that the different contexts in which the instruments have been proposed are considered: the draft Regulation has been proposed for general data processing, whereas the draft Directive applies in the field of police and judicial co-operation in criminal matters. The use of data in the areas covered by each instrument is very different and there is a need for greater flexibility in the field of police and judicial co-operation due to the operational requirements in this area and, where necessary, this should be reflected in the two instruments. Recital 10 of the draft Directive refers to Declaration 21 on the protection of personal data in the fields of judicial co-operation in criminal matters and police co-operation, which acknowledged that specific rules may be needed for the protection of personal data in this field.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, telephone, fax and email
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/general enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
Email: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Houses of Parliament Shop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/general enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: shop@parliament.uk
Internet: http://www.shop.parliament.uk

TSO@Blackwell and other accredited agents

ISBN 978-0-10-185302-6