Essex County Council

Response to the Department of Culture, Media & Sport call for views on the UK implementation of the General Data Protection Regulation (GDPR) derogations

Essex County Council (ECC) is a Public Authority serving 1.5 million residents and employing over 8000 staff. ECC offers a range a statutory services offered ranging from Social Care through to highways maintenance.

Theme 1: Supervisory Authority
Article 51 - Supervisory Authority **Article 53 - General conditions for the members of the supervisory authority** **Article 54 - Rules on the establishment of the supervisory authority** **Article 58 - Powers** **Article 59 - Activity reports** **Article 62 - Joint operations of supervisory authorities** **Article 90 - Obligations of secrecy**
ECC does not have any pressing views or evidence in regards to the above theme and derogations.
Theme 2: Sanctions
Article 36 - Prior consultation
Article 36 (4)&(5) allows for the UK Government to legislate for Data Controllers to consult with the Supervisory Authority in additional circumstances to that of 'high risk' and those outlined in Article 36 (1). Article 36 (5) specifically references Social Protection (Social Care) as an example where this could apply. ECC believes that further clarification should be given here as to exactly when this would apply, as all processing for Social Protection requiring prior consultation would slow up the process and devalue the point of having privacy by design. There therefore should be linked to the definition that is needed for 'high risk' processing.
Article 58 - Powers
ECC has no major concerns or feedback on this area other than to state that the powers outlined in Article 58 (1)(f), especially around access to premises, should fall in line with current UK law covering the rights and restrictions over powers of access.

Article 83 - General conditions for imposing administrative fines

Article 83 (7) allows for member states to lay down rules for when and how administrative fines are imposed on Public Authorities. ECC recognises that there is a need for the Public Authority to demonstrate compliance and be transparent with Data Subjects on their compliance however fines of up to £20million (or Euros) poses risks for the financial stability and ability to provide vital services should such a fine be imposed.

ECC would therefore recommend that an administrative fine 'system' for Public Authorities is developed which takes in to account the grounds for issuing of a fine as well as the lack of funds available to Public Authorities and that any fine issued simply moves tax payer money from one public purse to another. A balance should be struck between the need to enforce (the stick) and the recognition that funds aren't freely available to Public Authorities any more therefore a more proactive approach is needed (the carrot).

Article 84 - Penalties

Article 84(9) allows the UK Government to lay down additional rules and penalties with regards to any infringements of the requirements of the GDPR and derogations.

Currently under the Data Protection Act 1998 it is a criminal offence to knowingly and wilfully take or sell Personal Data without authorisation of the Data Controller (a section 55 offence). This can even carry with it a prison term in some circumstances.

ECC believes this provision is a vital protection and deterrent to prevent people from looking to steal Personal Data or try to engage in the Personal Data black market. As the GDPR is looking to offer more and better protections over Personal Data there should be something within UK law to prevent the theft and misuse of Personal Data, ideally by having this as a criminal offence.

ECC also believes that there should be further clarity within National Law as to the extent of Personal Liability for staff at any level should a breach occur, either knowingly or accidentally.

Theme 3: Demonstrating Compliance

Article 40 - Codes of conduct

Overall ECC believes that the creation of more detailed Codes of Conduct for aspects of the GDPR are welcome. We believe that focus should be placed on codes of practise in these respective areas and the codes should be endorsed / made in collaboration with an appropriate professional boy / trade association.

- Information & Records Management (in conjunction with standards outlined in the Public Records Act)
- Register of Processing Activities

- Breach reporting
- Data Protection Officer
- Subject Access Request
- Privacy Notices (including consent capture and maintaining)
- GDPR Risk Management (Information Risk)

Article 42 - Certification

ECC believes that the UK Government and Information Commissioners Office should pursue a GDPR Certification scheme, especially one aimed for those looking to provide services to Public Authorities. This should be designed to ensure that basic GDPR compliance is certified so that Public Authorities then do not need to perform the same checks on suppliers but instead can ensure their due diligence is for anything specific the provider in looking to do in that agreement. This will make it easier for suppliers to work with the public sector and also reduce the due diligence burden on Public Authorities as Data Protection is only one of many areas of 'legally required' due diligence, which often puts off suppliers from working with Public Authorities.

Article 43 - Certification bodies

While ECC has no major preference for how this is achieved we believe that in order for the Certification to have value, the certification criteria and those responsible for issuing certification should be separate (as happens with certification to ISO standards for example). Therefore if the ICO was to create the certification scheme and requirements, another body/bodies should via an official means (licensing for example), offer auditing and certification to that standard.

Theme 4: Data Protection Officers

Article 4 - Definitions

ECC does not have any views or evidence in regards to any conflicts in definitions with the requirements of the Data Protection Officer.

Article 37 - Designation of the data protection officer

ECC does not believe it is necessary for UK Law to impose any requirements on associations of local authorities under Article 37 (4).

ECC believes that in order to support the requirement of 'suitable qualifications' that the UK Government and/or Information Commissioners Office agree and publish a list of acceptable UK qualifications to hold. Currently there are numerous qualifications a DPO could hold with regards to Data Protection, including it being a subject in a wider legal degree. Some clear standards on the suitable qualifications (as a minimum for example) would offer a clear requirement and skills plan

for future DPOs.

ECC would also like to see some clarification on the standards under Article 37 (4) for clustering of entities to enable them to appoint a single DPO. ECC believes that many schools, voluntary bodies and smaller constitutional entities (parish and town councils) will not have the funds or resources to appoint a DPO for each entity therefore if they were able to cluster together to appoint one collectively per cluster.

Article 38 - Position of the data protection officer

Currently Article 38(5) believes that the the DPO's advice should be protected from disclosure regardless of whether or not the DPO holds a legal qualification..

Theme 5: Archiving and Research

Article 89 - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Under the current Data Protection Act 1998 the archiving condition (section 33) outlines the conditions for which this applies but also what requirements of the DPA do not apply in that processing purpose. Under the GDPR Article 89 (2)&(3) allow for the UK Government to legislate on outlining how the rights outlined in Articles 15, 16, 18, 19, 20 and 21 would apply to the Personal Data processed under these conditions / purposes.

ECC believes that this legislation should, at the very least, match the protections offered to archiving services under the Data Protection Act 1998. Some clarity would also be beneficial where there is no 'national statute' to archive information that is not deemed a public record but does have some historical (national or local) value.

Theme 6: Third Country Transfers

Article 49 - Derogations for specific situations

There is a gap under the current Data Protection law which is also not plugged by the GDPR. This relates to Subject Access Requests made by Data Subjects in other countries. There is a lack of clarity around data transfers if a Data Controller was to send the Personal Data to the requester knowing they would access it from a third country, likely to be an 'unsafe location'. While currently there are differing views and ambiguity under the GDPR we would prefer if this was made explicitly clear that it is or is not included in the third country provisions. And if not, what aspects of the request and subsequent processing are exempt.

Theme 7: Sensitive personal data and exceptions

Article 9 - Processing of special categories of personal data

We currently believe that as a Public Authority processing sensitive Personal Data for the purposes of Social Care (some under statute and some under consent) that the provisions in the below sections allow us to not rely on consent (for the services processed under statute).

Article 9 (2)(b) = processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

Article 9 (2)(h) = processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Social Protection Law as defined by the European Union, includes provision of Social Care and safeguarding, however in order to ensure this remains clear UK supporting legislation should define this and make it clear that statutory Social Services and Safeguarding purposes would come under this category.

We also believe the UK legislation should further clarify the processional secrecy protections outlined in Article 9 (3). For example, many professional involved in the provision of social care are under varying degrees of professional secrecy so some clarity on how this would interact with UK legislation on this area would be beneficial to all concerned.

Theme 8: Criminal Convictions

Article 10 - Processing of personal data relating to criminal convictions and offences

The GDPR currently does not offer protections over the processing of Personal Data for the prevention and detection of crime. If the Data Protection Act 1998 is repealed this will leave a gap in the protections and requirements of the processing of Personal Data for this purpose. ECC therefore believes that legislation should be drafted to cover this gap and that at the very least the same protections and requirements of the DPA should be in place.

This could include, but is not limited to, ensuring that the prevention and detection of crime is a clear ground for processing, that does not require data subject consent. This would also include provisions around Section 29 & 31 requests and how they would now need to interact with the GDPR requirements, again maintaining a need to not notify or seek consent of the Data Subject when processing or responding to the request.

We also believe that within the employment processing related legislation, there should be clear provisions around the processing of Special Categories of Personal Data for the purpose of DBS checks. Currently we believe the provisions in the GDPR for this are too vague, especially where

the processing concerns criminal record information.

ECC would like to stress the impact of not getting it right would significantly affect various important aspects of Public Authority operation. Including, but not limited to, our duties for safe guarding, adult and child social care, multi-agency cooperation, efficient and effective processing of care proceedings, supporting troubled families and responsibilities under trading standards.

Theme 9: Rights and Remedies

Article 17 - Right to erasure ('right to be forgotten')

ECC believes that the definition used in Article 17 (3)(c) for 'public health' should be clearly defined, as there are several functions that the UK calls public health that would not seem to meet the implied definitions under the GDPR.

Article 22 - Automated individual decision-making, including profiling

Profiling is often undertaken with regards to the provision of public services, especially within a Social Care context in order to determine the care package appropriate to their needs or determine their level of risk to a member of staff or other individual based on any specific needs or behaviours. Currently Article 22 states that Data Subject's cannot object or withdraw consent where the profiling is enabled by member state laws. While some of our statutes, for example the Care Act 2014, will outline the need for what is referred to as profiling under GDPR; other statues are older and will need revision especially in the provision of Passenger Transport.

Article 26 - Joint controllers

Under the GDPR we are losing the definition of 'Data Controllers in common'. This was very useful in situations where the point of data collection could be the same, but the purposes for each controller were very different. For example, in an application for assistance, the assistance may be offered by 2 different entities especially if one aspect of the care assistance requires specialist experience. Under the GDPR we would need to, in that arrangement, be joint controllers for everything we both collect together or separate out the data collection so it is clear they are very different. In a social care context this can be very confusing for data subjects result in unnecessary complexity and then means that we need to police each other in what we are doing with that Personal Data..

ECC therefore believes that any derogation law should outline a suitable definition that allows for Data Controllers in common (including outlining that they can be responsible for different purposes and not each other's).

Article 80 - representation of data subjects

ECC does not have any pressing views or evidence in regards to the above theme and derogations.

Theme 10: Processing of Children's Personal Data by Online Services

Article 8 - Conditions applicable to child's consent in relation to information society services.

ECC believes that UK legislation should allow for the age of consent to be lowered to 13, as allowed under Article 8 (1). We also believe that some provision should also be made for the current Gillick competency test so that should a child of below 13 years of age, engage with council services that are offered by various means, including online, the processing would not require consent if they are deemed to be Gillick Competent. Our concern is that having different standards with regards to when child consent is needed and what that consent is, especially in the context of any online care, counselling or medical support, may lead to conflicts between different areas of UK legislation which may then also affect the ability to act in the child's best or vital interests.

Theme 11: Freedom of Expression in the Media

Article 85 - Processing and freedom of expression and information

ECC does not have any pressing views or evidence in regards to the above Article 85 and its derogations.

Theme 12: Processing of Data

Article 6 - Lawfulness of processing

Overall, ECC does not have any pressing views or evidence in regards to the above Article 6 and its derogations. However we do believe that the derogations for the processing of Personal Data for employment purposes should be in place as soon as possible. This should include provisions for processing of personal data for payroll purposes clearly outlined as part of employment processing purposes.

Article 18 - Right to restriction of processing

Similar to theme 13 below, ECC believes that it should be made clear in UK law that where processing is done under the grounds of statute, where original records of Personal Data are

needed to verify compliance with those obligations, rights to restriction, deletion or correction cannot apply either fully or in part. More information on each restriction is outlined in theme 13.

Article 28 - Processor

ECC does not believe that any further UK derogation outlined in Article 28 (3) & (4) would be required beyond what is currently allowed by UK law. Article 23 (3) currently outlines what a data processing agreement should contain and currently there are sufficient standards in UK contract law to define what a contract is and how it should be enforced.

ECC does welcome and encourages the creation of a Code of Practice for Data Processors. We believe that this will assist in raising awareness of Data Protection amongst processors and suppliers, and in conjunction with a certification scheme will assist Data Controllers in managing large and diverse supplier portfolios.

Article 29 - Processing under the authority of the controller or processor

ECC does not have any pressing views or evidence in regards to Article 29 and derogations.

Article 32 - Security of processing

With regard to Article 32 (4), ECC does not have any pressing views or evidence in regards to the above any further derogation needed in this context above current UK law.

Article 35 - Data protection impact assessment

With regard to Article 35 (10), ECC does not have any pressing views or evidence in regards to the above or any derogation needed in this context.

However, with regard to Article 35 (4) & (5) we believe the supervisory authority should move quickly to publish a list of what sort of processing would require a DPIA, including a clear definition of what would be classed as ‘high risk’ processing in their view.

Article 37 - Designation of the data protection officer

With regard to Article 37 (4), ECC does not have any pressing views or evidence in regards to the above or any derogation needed in this context.

Article 86 - Processing and public access to official documents

ECC believes that changes in guidance and possible Freedom of Information Act 2000 wording are

required in order to ensure that the FOIA continues to interact well with the GDPR and any UK supporting legislation for employment and crime data processing. As a public authority subject to Freedom of Information requirements it is important that this is implemented from 25 May 2018 so that we can continue to meet both our GDPR and FOI obligations. Currently there is the possibility for some confusion, especially as the definition of Personal Data (and special categories) is now far wider than the current DPA definition.

Article 87 - Processing of the national identification number

Currently the UK does not have a national ID number, outside of a National Insurance Number or NHS number. Therefore, with regards to Article 87 (1), ECC does not have any pressing views or evidence in regards to the above or any derogation needed in this context, other than to ensure current standards are maintained.

Article 88 - Processing in the context of employment

Currently, the DPA is not clear on employment contracts and the provision of a clear consent. Where processing is required by law, consent is not needed and that should continue to be the case. However where processing is required in order to employ someone, manage their employment and manage their ongoing training and development, under the GDPR definitions, consent given in an employment contract would not be valid. It is ECC's view that a UK derogation on employment processing should make it clear that the legal grounds for processing is the provision of employment by contract and then outline steps that an employer would need to take to balance that lack of 'effective consent'. This could include requirements on what to include in an employment contract or notice through to outlining what information is and is not needed to meet basic employment purposes. This may therefore require changes to employment related laws to make this clear.

Theme 13: Restrictions

Article 23 - Restrictions

ECC believes that the restrictions and 'exemptions' of the Articles 12 to 22, 35 and 5 should, in so far as possible, offer at least the same exemptions as the current Data Protection Act.

ECC also believes that any restrictions/exemptions should be limited to purpose only (and not entity or sector). To take the NHS as an example, where there is a dependency on health data to provide statutory care and other purposes, to have a restriction / exemption in place for one entity but not the other has the strong potential to double the compliance requirements. Especially if information is recorded in a way that would be incompatible with GDPR requirements on notifications and consent. Wherever possible, these requirements should be the same or work in conjunction with each other.

For each Article we have summarised the key requirements below;

Article 5: Principles
The DPA currently allows for elements of the principles to not be applied to processing where certain conditions are in place. For example, if an accusation of crime has been suspected and it is not permitted under law to advise the accused at that point, you can therefore not advise them that you are processing such data on them and indeed sharing it (anti-money laundering being an example). Any UK derogations should therefore mirror the exemptions outlined in the DPA currently.

Article 12: Transparency
Similar to the above, any UK derogations should align in this area to the above as well as offer similar protections to Data Controllers when processing personal data for those purposes.

Article 13: Information provided to Data Subject if collected directly
Similar to the above, any UK derogations should align in this area to the above as well as offer similar protections to Data Controllers when processing personal data for those purposes.

Article 14: Information provided to Data Subject if collected indirectly
Similar to the above, any UK derogations should align in this area to the above as well as offer similar protections to Data Controllers when processing personal data for those purposes. ECC also believes that limitations on the extent of this requirement should be placed. For example, in a social care context it is often the case that Personal Data on a neighbour of a data subject that may collect their shopping for them in captured in a Social Worker assessment of care need. Under the GDPR we would then be processing that neighbours information, would we then need to inform them of this? Given the resource implications this has we don't believe this has any value either for the Data Subject concerned or our obligations under the GDPR.

Article 15: Right of Access
Under the Data Protection Act 1998 the below exemptions from providing Personal Data in a Subject Access Request are believed to be important in order to protect various interests.

Schedule 7(10) – Legal Professional Privilege; This is vital for protecting the legal professional privilege rights under current UK law and ensuring that legal advice can be sought on matters relating to data subjects and not be automatically released without due care and attention to the above. While there are provisions in the GDPR to protect professional secrecy we believe supporting UK legislation should supplement this and make it clear how it would operate for the UK.

Schedule 7(1) – Confidential References; As a public authority providing Social Care services to adults and children we rely on references and 'statements' being provided by third parties of various natures. These references often cannot and should not automatically be disclosed to the Data Subject concerned due to their content. Often the content may be something distressing to the individual or will often contain the personal data of the person providing the reference. Due care should be given and allowed under Data Protection Law before such information is freely provided to the Data Subject. Currently we do not believe the protections offered in the GDPR are clear enough to offer this level of protection.

Section 38 (2) - Information requested under another enactment; We often receive requests for Personal Data that often come under the provisions of other UK legislation, for example the Access

to Health Records Act . We do not believe that the GDPR offers a suitable gateway to make it clear to Data Subjects that their information/request is not being processing for that purpose under the provisions of GDPR.

Section 30(3)(b) – Health and Social Work exemption; Where some elements of Personal Data are being processed for the purposes of Health & Social care and it is not in the best interests of the Data Subject for the provision of that care for some elements of their care record to be available to them, this exemption means the authority can consider appropriately the impact on the care provision and data subject before the information is or is not released. The provisions in the GDPR currently do not provide appropriate protections from access for this purpose.

Schedule 7(7) – Intentions in regards to negotiations; In particular circumstances, especially in the cases of employment tribunal / disciplinary, it is important that employment files are given due attention and review before being released to an employee. Where a case is particularly sensitive or complex, as with cases before a court, asking for information early or more information wider than just the matter at hand can often disrupt the proceedings and not allow the appropriate (and often legally required) processes to take place. UK legislation either here or in the Employment processing laws should outline how this right to access works with regards to current or ongoing employment negotiations.

Schedule 7(5) - Management Forecasts; A number of Subject Access Requests will ask for copies of structure charts or forward plans for staffing where their personal data is included. Often these plans are draft, have an element of commercial secrecy to them or, under UK legislation, should only be disclosed to the staff concerned at certain points (especially if job roles are changing). Currently the GDPR does not offer a provision to allow Data Controllers to consider this before responding to a request. UK legislation should therefore outline how this right to access interacts with other such legal requirements surrounding draft documents, staff planning and management forecasts.

Based on the issues experienced with the current Data Protection Act we believe that it would of beneficial use for us and others for the UK Government to include the below provisions on any UK supporting legislation.

Vexatious Requests; as with Freedom of Information Legislation, we receive requests from individuals that are vexatious in nature either in frequency, behaviour, or purpose. The provisions under FOI allow for authorities to consider the circumstances around the requests from the requestor and determine whether or not someone is being vexatious. If UK legislation was to offer some mechanism for Data Controllers to determine if a Data Subject is being vexatious, for example if they ask for weekly SARs on any changes to their record made that week, it would help prevent pointless requests that do not serve the rights and freedoms of either the Data Subject or the Data Controller.

Information yet to be recorded; In the Social Care context we are often asked for information from a Data Subject before the information is recorded into a relevant filing system. For example, a

summary may be written in rough note form on a Monday and a request is made by the Data Subject for that information on the Tuesday. That information, in its rough form is not 'data' as defined by either the DPA or GDPR therefore is not releasable under SAR. However the Data Subject knows it exists therefore will complain or become confused about how Data Protection legislation works. We believe therefore there should be provisions in the UK legislation on how to process these requests and what rights both Controllers and Subjects have over such notes.

Article 16: Right of Rectification
Any restrictions on the right to rectification should offer the same level of protection as the Data Protection Act 1998. For example, where information on a care need referral was recorded on the day the referral was made, which then turns out to be inaccurate for one reason or another, we as the Data Controller and entity responsible for responding to that care referral need to be able to demonstrate that appropriate actions were taken based on that information. There therefore needs to be an exemption to the right to rectification (and erasure) that allows Data Controllers to continue to process that original record for those purposes but ensure that it is not used for other purposes (like delivery of current care needs for example).

Article 17: Right of Erasure
Similarly with Article 16 above and 18 below, any restrictions on the rights on erasure, rectification or restriction should interlink where the processing by the Data Controller is based on statutory requirement. Any derogation should make clear that what Personal Data remains exempt is defined and evidenced by the Data Controller as being needed in order to demonstrate compliance with that statute and/or statutory duties.

Article 18: Right to Restriction
Similarly with Article 16 and 17 above any restrictions on the rights on erasure, rectification or restriction should interlink where the processing by the Data Controller is based on statutory requirement. Any derogation should make clear that what Personal Data remains exempt is defined and evidenced by the Data Controller as being needed in order to demonstrate compliance with that statute and/or other statutory duties.

Article 19: Notification of Right to Erasure
ECC believes that where, in Article 19 (1), the requirement to notify other entities of a requirement to delete personal data use the term 'disproportionate effort', this should be clarified either in guidance, codes of practice or derogation legislation. As a provider of a range of services, some of which involve other partners and suppliers, if a requirement was to inform each and every provider and third party, this would involve a lot of effort and take longer than a 20 day period (for example). We believe that it should also be outlined where responsibility lies for the request to delete being enforced. I.E., if a request is not actioned by a third party that we have informed, what responsibility do we have over that as the controller that first received the request?

Article 20: Right to Data Portability
With regards to Article 20, ECC does not have any pressing views or evidence in regards to any restrictions on the right to Data Portability outside of what is outlined in Article 20 other than that the right to receive this information should be subject to the same restrictions as any other COA. It may be worth, however, ensuring that in supervisory authority guidance there is clarity that processing under enactment is exempt from the rights in Article 20.

Article 21: Right to Object
With regards to Article 21, ECC does not have any pressing views or evidence in regards to any restrictions on the right to object outside of what is outlined in Article 21 and providing other

requirements outlined for grounds for processing and profiling, outlined above, are adopted.

Article 22: Automated Individual Decision Making & Profiling
As with the above, with regards to Article 22, ECC does not have any pressing views or evidence in regards to any restrictions on the right to object outside of what is outlined in Article 21 and providing other requirements outlined for grounds for processing and profiling, outlined above, are adopted.

Article 35: Data Protection Impact Assessment
Similar to theme 12 above, it should be made clear by the supervisory authority what situations require a DPIA to be completed, and therefore by implication which ones do not. It should also be made clear where and when consultation with Data Subject's would be appropriate and when not.

Theme 14: Rules surrounding Churches and Religious Associations

Article 91 - Existing data protection rules of churches and religious associations

ECC does not have any pressing views or evidence in regards to the above theme and derogations.

Additional question: cost impact

In the context of the derogations above, what steps should the Government take to minimise the cost or burden to business of the GDPR?

Local Government is subject to unprecedented budget pressures arising mainly from social care, inflation (including the national living wage), and reduction in central government grant. It is therefore important that any additional costs arising from GDPR should be funded by central government. Costs can be minimised through early decision making, allowing local authorities time to plan and implement properly. Efficiencies can also be realised through making best use of processes already in place, and reducing unnecessary beaurocracy. We would be happy to work through this on more detail.