# Chapter Six – Impact on your organisation

Date – 17.12.21

## Q6.1.1. What compliance activities does your business currently undertake as a result of the UK GDPR and DPA?

* Seeking legal advice? Yes.
* Establishing a legal basis for data processing or acquiring consent? Yes.
* Responding to Subject Access Requests? Yes.
* Responding to consumer complaints? Yes.
* Notifying data breaches? Yes.
* Other compliance activities or record keeping? Yes.
* Preparing DPIAs? Yes.
* Any other? Not applicable.

### Q6.1.1a. If you selected 'Other' please provide more details

Not Applicable

### Q6.1.1b. What do these compliance activities cost your organisation in time and money?

Organisations in GM have not costed this out as they are mostly embedded as part of the organisations business as usual activities. There is a high cost, and more importantly time element to managing compliance for some organisations as often there has not been in the investment in the good foundations to build monitoring off. Often seen as a nice to have rather than a core capability.

Within the VCSE sector it is recognised that compliance has a significant cost that many struggle to meet due to the funds available to them for business activities beyond their charitable/voluntary purpose.

As one example of the time that compliance activities take, DPIAs were looked at by the project team for Dapian a Digital DPIA tool. In this exercise it was estimated that a single word processed DPIA assessment would take on average 72 hours. It was calculated that this equated to £1,928.57 based on a Grade 5 pay grade in a Local Authority. The project created the Dapian Digital DPIA tool, and these figures then reduce to 26 hours per digital DPIA and a cost of £696.43 per Digital DPIA. [The Dapian Business Case](https://dapian.uk/business-case/)  shows that with investment by the organisations in how data protection requirements are undertaken the burden is much less. In both times, spent by the organisation but also money.

Similarly, it is recognised that documenting flows of data between organisations in data sharing agreements is a costly process in terms of time, and the number of organisations involved in each data sharing instance, along with the number of often senior staff involved in review and sign off of each agreement from each organisation. In a manual process this would involve multiple versions of documents being sent around several individuals and organisations which can lead to confusion and takes a significant amount of time to complete sign off. Cumbria Partnership NHS Foundation Trust and its partners developed an [Information Sharing Gateway](https://www.informationsharinggateway.org.uk/about) digital tool to support the creation of sharing agreements which can be accessed by all partners for review and sign off electronically which reduces this, but also provides a way of recording all sharing agreements in one place. It was calculated that manually completing sharing agreements takes 2 days – 1 week; manually retrieving an agreement up to a day and signing off an agreement around 100 hours. With the use of the ISG these timescales are reduced to 1 hour – half a day to draw up the agreement, 1 minute to retrieve an agreement, and approximately 1 day to obtain sign off. Again, this is another example of how investment in enabling the business with appropriate tools lessens the burden on organisations.

There is still an impact in terms of the number of agreements being developed, and this will continue even if the proposals are implemented. For example, GMCA currently has more than 250 data flows logged in the ISG (including those in draft). The Information Sharing Gateway is widely used within Greater Manchester in the public sector.

## Q6.1.2. We would like to understand more about how (if at all) your organisation would be affected by the measures outlined in the consultation, specifically:

## What compliance activities would change as a result of the measures?

## What other impacts would the proposed measures have on your organisation?

It is unlikely that there would be a significant cost/time benefit to some of these changes. For example, Local Authorities are large complex organisations who would need to continue with a number of the activities which are being proposed for change. This would particularly relate to accountability activities which would remain a requirement regardless of the form they take e.g. the removal of a requirement for a DPIA would have a net zero benefit as accountability documentation would still need to be in place for any new/changed activities.

One clear benefit is explicitly allowing processors to use the same legislation as the controller for their processing activity, as this would reduce the time local authorities currently spend negotiating the legal basis with third parties. However, as a group we were unsure as to whether this needed to be addressed within the legislation (which does allow for processing under public task by any kind of organisation) or whether clearer guidance would suffice.

There would also be an impact where processes such as DPIA completion or the Record of Processing Activities are removed (for example) as considerable work has been undertaken since 2016 (when the GDPR text was approved) to embed these practices within organisations. If all of the proposals are brought forward this would create uncertainty with non-information governance employees, and undermine the work completed for the organisation to manage risk and show accountability. In addition, it was felt by some organisations that the changes may not be big enough to justify a change so soon after GDPR came into effect.

It was also recognised that in some organisations (particularly within the public sector) DPIAs have been in use since before the development of GDPR as good practice, and some organisations already require DPIAs to be undertaken for more than just the activities which are required to have one by law. This can prove onerous for smaller organisations to provide where organisations require a DPIA to be completed for delivery of particular services. Some organisations confirmed that they were unlikely to remove the requirement to undertake DPIAs since they proved to be a useful tool to document responsible use of data, engagement with the public and aided due diligence and accountability tasks.

There would also be significant monetary and resource (time) cost in updating training materials in order to educate organisations fully regarding the changes. This goes even further for charities and voluntary organisations where there is little money available to deliver training. For these organisations there is a need not only to educate the wider workforce, but to ensure those individuals with direct responsibility for compliance activity have the skills, policies and confidence required to deliver a compliant organisation.

## Q6.1.3. How (if at all) would the proposed measures affect your organisation’s collection, use or processing of data?

Local Authorities are creatures of statute and required to undertake a wide range of functions by law. There are a small number of areas that would have a beneficial impact:

* simplifying the rules relating to Cookies
* simplifying the approach to information sharing and lawful basis
* simplifying the arrangements for CCTV but only if the documentation requirements became less onerous

Charities and private sector organisations may find it easier to work for public bodies, or alongside them where clarity is provided regarding the applicability of the public task lawful basis.

## Q6.1.4. We would like to understand more about how (if at all) international data transfers your organisation carries out would be affected by the proposed measures, specifically:

## What is your current reliance on and opinion of alternative transfer mechanisms?

Some organisations who have contributed to the Greater Manchester response to this consultation felt that the changes proposed may have a detrimental effect on adequacy decision from the EU which could have an impact on the ability to transfer data to the EU. This would in turn have an impact on organisations who currently routinely transfer data to the EU as all the existing arrangements would need substantially updating which would take significant amount of time and legal resource in addition to information governance resource.

### What impacts on your organisation do you expect from the proposed measures?

 We would expect clarity on areas mentioned in the consultation either in the form of updated consultation and/or further guidance from the government and ICO.

We would also expect to see a single assurance mechanism for all data protection activity e.g. if the Council develops a compliant PMP, this should be accepted as assurance for all compliance regimes e.g. The health data security and protection toolkit, assurance requests from Government Departments or their suppliers in relation to specified funding/activities. Local Authorities spend time responding to requests for assurance from other parts of the public sector and their supplier asking similar questions.

As expressed in multiple responses throughout our response, we feel that some of the proposals will weaken trust from the public, which would present a challenge in terms of being able to deliver research or other business outcomes which require a positive opt in from the public. It may also lead to a rise in information rights requests (under both data protection and freedom of information legislation) as the public seek to find out more about what the organisation is doing with their data.

It was clear during discussions on the use of data during the initial stages of the Covid-19 pandemic, that it was not clear to some organisations and members of the public that there was already a lawful gateway to allow sharing of personal data, or indeed to mandate it (through the COPI notice). It was felt that there needed to be more guidance and publicity on the lawful bases for sharing personal data, not necessarily from within the Data Protection legislation, but also more widely about the existing legislation available to facilitate processing of personal data in specific circumstances. In the past, the view expressed by the ICO is that lawyers within the business will know the legal basis for the entirety of the organisations’ tasks (particularly within the public sector), but in our experience this is not always the case. It would be useful for government to assist with identifying legal bases by providing and updating a central list of legal gateways which can be relied upon. This would greatly reduce the burden on organisations to identify and negotiate the lawful basis in use. Where there are perceived blockers, it may be the case that the issue lies in the legislation outside the data protection act, and that targeting that legislation would assist in removing the blockers.

It is worth noting that for most of the organisations involved in this Greater Manchester Response, removing the requirement for organisations to appoint a Data Protection Officer is unlikely to have much of an impact. In Local Authorities, Housing organisations and VCSE organisations it is likely that the role of the DPO will remain, as organisations will need an individual to take responsibility for compliance and accountability in whatever form is required. The only difference may be the role the individual takes within the organisation, or the role title. Similarly, it is highly likely that most organisations would continue to complete DPIAs as a policy so that organisations can document the personal data processing taking place. It is expected that as now, the ICO would request to see a copy of a DPIA in the event of a data breach to demonstrate that the system has been assessed for data protection compliance and any associated risks appropriately mitigated. As a result, the cost of undertaking DPIAs either digitally or word processed would stay the same (see top).