DPA Somalia implementation: the requirements to achieve full compliance

Somalia's Data Protection Regulation (DPR) is legislation that is designed to protect the data of Somalia citizens. DPR implementation affects every single organization and business that interacts with in Somali, regardless of where they may be located.

Table of contents

What is the Data Protection Regulation?

The Data Protection Regulation was enforced across the Somalia on March 23th, 2023. The goal of this legislation is to protect the information and privacy of all individuals that reside within the Somalia, requiring businesses to offer greater transparency into how a person's data was collected, used and stored.

How to implement DPR in an organization

Now that you have gained a brief understanding of the severity of compliance deviation, you may be wondering about how to implement DPR in an organization.

To help with this, we have collated four main actions that you can take to kick start this obedience of regulations. They are as follows;

1. Raise awareness
In order to achieve DPR implementation, you must first ensure that everyone within your organization has a strong understanding of what data protection is and its importance.

To achieve this, you should consider offering training sessions to all employees, followed by a concise, mandatory exam on completion. This can include a comprehensive understanding of the topic, best practices and scenario based activities. By doing this, you can directly measure a person's understanding of the concept and improve upon specific areas.

It is imperative that all employees have a comprehensive understanding of the consequences for non-compliance, both individually and on an organizational level.

2. Create a data inventory
Gaining an understanding of the data that your organization collects and processes is an important step in ascertaining the risks associated with information processing, storage and transferal.

Once the list of data types has been compiled, including customers, employees, suppliers, etc., you should begin to map each set of data's end-to-end journey throughout your business infrastructure. This way, you can successfully identify all the physical and virtual places where this data has held a presence.

These lists can then be distributed to departments within the company, and stakeholders, in order to ensure that all data types and location have been correctly recognized.

3. Risk evaluation
Having taken inventory of your data and processes, it is now time to evaluate the risk associated with your practices and compare these to the existing DPR requirements.

In doing this, remember to include all third-parties involved in your organization, such as vendors or suppliers.

To undertake a risk evaluation, consider these questions;

- Where do the gaps in our compliance exist?
- What areas are at threat of non-compliance in the future?
- What are the immediate needs that must be addressed in order to progress our DPR compliance?

4. Develop a roadmap
This will outline the entirety of the processes and system changes that need to be made in order to achieve full conformity with regulatory requirements.

What are the consequences of non-compliance with DPR requirements?

The initial consequence for companies that fail to abide by data protection ruling will be monetary. There are two tiers of maximum administrative fines that exist as penalties for non-compliance, which are

- 2% of annual turnover
- or 4% of annual global turnover

In short, failing to follow the DPR compliance requirements will force your business into a problematic situation and ultimately damage your organization. The punishments are intentionally harsh to ensure that all organizations follow a DPR implementation strategy.

How can I prepare my organization for DPR implementation?

In order to make it easier for your business to follow the DPR compliance requirements, it's essential that you start planning ahead of time while you still can. To help you prepare for DPR implementation, we have outlined several of the most important points to follow.

1. Audit and analyze your data
Data regulations should not be seen as a curse for businesses, but rather as an opportunity to improve the quality of the data collected.

Here are a few questions you should ask yourself:

- Who are we collecting data on? Who has access to this data? Who is the one that sorts it and compiles it into usable data?
- What are we collecting? What kind of safeguards and mechanisms do we have in place to protect personal data so that it isn't leaked into the wrong hands?
- When are we collecting data? How long do we plan to keep it for? Are we going to share the information we have with others?
- Where are we keeping data? Is it stored and compiled automatically, or do we transfer it all to a third party?
- Why are we collecting data? Do we feel that the information we collect is useful? Is it being used for a good reason?
- How are we collecting data? How do we plan to process it in the future? How long do we keep our data for?

These questions should form the basis of any organization's DPR implementation strategy.

2. Inform customers about DPR
Another important step towards safely managing personal data is to be transparent with your own customers. DPR can be used as a source of differentiation for your organization, as it is viewed as a positive attribute by the public.

Transparency is critical in building trust between companies and consumers.

Customers have become knowledgeable about data protection rights and the risks associated with the misuse of their information. Therefore, you should consider making it common practice to reassure customers of how you go about effective DPR implementation.

3. Review privacy notices

The DPR compliance requirements contain a list of requirements that all privacy notices must meet should you collect data. This includes the following:

- Indicate the processing activities taking place anytime you collect personal data
- If personal data isn't being obtained directly, then inform what processing activities are taking place
- Notices must be present whenever personal data is collected and at all points
- Data must include the identity of the controller and of the data protection officer, how long it will be kept for, the rights that the consumer has, the right to file a complaint, the recipients and transfers of data, a statement that the consumer has the right to withdraw consent at any time, and also an explanation of why you or third-party wishes to collect the data.

4. Understand consumer rights

To follow the DPR compliance requirements, it's also important to understand the rights that the consumer has over their data.

When DPR implementation is active, you must demonstrate that you're able to do the following:

- Confirm the identity of whoever is requesting the data
- Give consumers the ability to request their personal data
- Respond to requests for access to personal data
- Trace and search for a consumer's personal data and deliver it within 30 days
- Request rectification and rectify any personal data collected
- Request the deletion of a consumer's personal data
- Understand which additional controllers data has been transferred to
- Upon a data breach, contact those entities to delete the data
- Requesting the restriction of data processing and showing how and when this is done
- Requesting copies and transmitting personal data
- Find personal data and compile it into machine-readable formats
- Give consumers a way to object to their data being collected
- Stop all data processing and demonstrate their compliance

These are the standard rights that must be understood by all organizations that follow the DPR compliance requirements. Failing to do so will result in heavy fines, so make sure you understand these points.

5. Learn how to run DPR-compliant marketing campaigns

An important aspect for companies is to align with the new DPR guidelines and responsibilities on the major advertising platforms, such as Google and Facebook.

If your organization runs marketing campaigns on Google, you should examine in-depth your responsibilities as a data processor or data controller.

6. Keep your audiences updated based on consensus
One of the requirements for companies to be DPR compliant is to make sure that the audiences targeted for marketing purposes are always updated according to the user consensus to be targeted.

This must be ensured both for new contacts and for contacts who expressed their consent before March 23th, 2023. In fact, according to the DPR "*if the consent provided by a person prior to the application of the Data Protection Regulation (DPR) is in line with the conditions of the DPR, then there is no need to ask again for the individual's consent.*"

Users have also the right to withdraw their consent at any time, and companies should respect their decision by excluding them from any marketing campaigns. This can be challenging especially for large organizations that deal with high-volume audience segments in hundreds of active campaigns, which could never update the audience's files manually every time people withdraw their consent.

7. Improve privacy-related internal procedures
The implementation of DPR and generally any data-protection regulation also affects companies' internal procedures. In fact, as regulations around personal data management increase, companies experience longer bureaucratic internal procedures.

Usually, in large organizations, data protection is regulated by the legal department who make sure to meet quality standards and data hygiene.

8. Appoint a Data Protection Officer
Another means of how to implement DPR is to appoint a data protection officer. This is required in any company that processes information and data on a large scale. They will need to do the following:

- Maintain audit trails and demonstrate accountability and compliance
- Maintain an inventory of data that categorizes consumers
- Maintain auditable trails of the processing activity
- Carry out data protection impact assessments
- Monitor compliance with data protection laws
- Liaise and assist supervisory authorities.

Failing to follow these DPR compliance requirements could result in harsh punishment, so you'll need to either hire a new employee or assign an existing one to this role. Because of the training required, it will be wise to do this as soon as possible as part of the DPR implementation process.

9. Enabling data transfers
The DPR compliance requirements state that consumers must have the ability to transfer data to themselves whenever they want. This means that you will need to return their

personal data at any given time, so you must be fully capable of compiling the information you have on each consumer into a machine-readable format. This way, you can easily transfer their data to another data controller.

If your consumers want their data, then you need to oblige and send it to them in a simple and readable format that they can understand. You will need to speak with any software engineers or technology consultants you hire in order to build a DPR implementation strategy that allows for this easy transfer of data. Failing to follow this could breach the DPR compliance requirements and result in a fine.

10. Planning for data breaches
Data breaches can create huge legal, financial and reputational upsets that could damage an organization and must be avoided when developing a DPR implementation strategy.

As such, it should come as no surprise that data security is an important consideration in the DPR and it requires that you follow the appropriate procedures when learning how to implement DPR compliance.

- You must be able to provide mechanisms to pseudonymize, encrypt and secure personal data
- You must implement additional security measures
- You must be able to confirm ongoing confidentiality, integrity, and availability of personal data
- You must provide mechanisms to restore access and availability of personal data
- You must be able to facilitate regular testing of your security measures
- You must be able to notify the data protection authority within 72 hours should you experience a data breach incident
- You must be able to notify the affected consumers should a high-risk data breach take place

Data breaches can create huge legal, financial, and reputational upsets that could damage an organization and must be avoided when developing a DPR implementation strategy. As part of your data security measures, it is essential to establish and maintain an internal audit process to regularly assess and evaluate the effectiveness of your data protection measures, identify any vulnerabilities, and ensure compliance with DPR requirements.

What are the DPR audit requirements to consider?

Understanding the requirements and present processes of effective DPR implementation is imperative. By deciphering this, you can identify any gaps that are present in your compliance.

Conducting an audit is a streamlined, concise method of assessing these factors, and should be conducted in order to maintain standards.

The following headings should be viewed as DPR audit requirements that must feature;

- Data governance
- Risk management
- DPR project
- Role and responsibilities arrangement in your organization
- Scope of compliance
- Analyze the procedure
- Personal information management system (PIMS)
- The rights of data owners (subjects)
- Information security management system (ISMS)

Carrying out your audit under these headings is the most effective means of proving the DPR compliance of your company.

What should be included in a DPR audit checklist?

You must keep in mind that any audit will be dependent on a number of factors, which can include the scale of your operations, the type of data you collect and the results of your data protection impact assessment.

Having established the requirements of your compliance analysis, let's take a look at the key components of a DPR audit checklist

Personal data and data subjects categories
You must list the categories of personal data and data subjects that you have collected.

This includes employee data (both previous and current), customer data (including sales information), information from within your marketing database and any CCTV camera footage that you may have collected.

Personal data elements included in data categories
It is mandatory to list each type of personal data that is included within singular personal data categories.

This includes names, addresses, banking details, videos, images, browsing history and purchasing history.

Personal data processing purposes
You are required to list the purposes of personal data collection and retention within each data category.

This includes research, systems integrity, HR proceedings, advertising, marketing, product development and service enhancement.

Legal basis for each processing purpose
For each purpose that personal data is processed, you are required to list the legal basis on which the process is based.

This includes consent, contract and legal obligation

Special categories of personal data
If there are special categories of personal data that are collected and retained, you must establish the details of the nature of this data.

This includes health, genetic and biometric data.

Legal basis for processing special categories of personal data
It is mandatory that you list the legal basis on which special categories of personal data are collected and retained by your organization.

This includes explicit consent and a legislative basis.

Retention period

For each category of personal data, your organization must list the period for which the data is intended to be kept.

It is important to note that there is a general rule in which data must not be retained for longer than is necessary, considering the purpose of why it was collected.

Action required to be DPR compliant

Finally, you must identify any actions that are required to be undertaken in order to ensure all personal data processing operations within your business are DPR compliant

This may include deleting data that no longer serves a purpose.