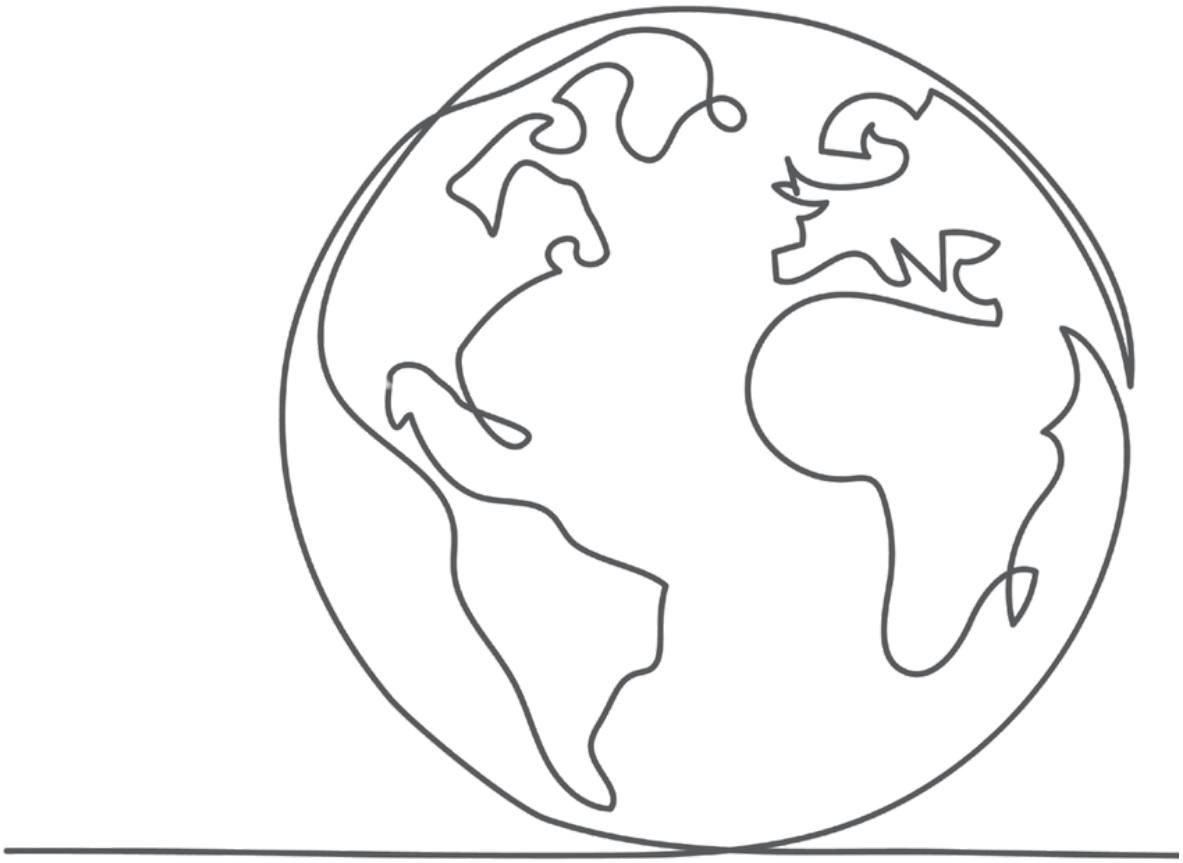
THE OFFICE OF THE
Data Protection
Authority

GUIDANCE: ESG / Sustainability reporting



2024 issue

ESG / Sustainability reporting

Summary

This guidance is for organisations that collect personal data as part of monitoring their environmental, social, and governance (ESG) factors. It is intended to help you understand how these interact with the legal obligations contained in *The Data Protection (Bailiwick of Guernsey) Law, 2017* ('the Law').

The Law exists to protect individuals' rights over their personal data (facts or opinions about or related to them). The Law contains seven principles that all local organisations are legally obliged to adhere to whenever personal data is involved.

Before we cover the seven principles, let's first look at three aspects you should consider at the outset with regard to ESG reporting: data collection, risk to individuals, and public disclosure of data.

1. ## Data collection

   It is unlikely that there are any ESG reporting obligations that **compel** you to collect information that is linked to an identified (or identifiable) living person. So, wherever possible, you should **collect information from people anonymously**. If data is *genuinely* anonymous the Law does **not** apply – as anonymous data is not personal data. You can therefore save yourself a lot of time and effort simply by collecting anonymous data instead of personal data. For data to be considered anonymous you must have **no way of connecting any information to a particular person**. It is important to note that this is different to the concept of 'pseudonymising' data[1] where you separate the identity from the data but retain the ability to join it back together, for example, by using a key.

   However, there may be circumstances where data is collected in a way that is deliberately (or inadvertently due to small sample size) linked to identified (or identifiable) individuals. In these circumstances you are collecting personal data and you need to take account of all the legal obligations the Law places on you, in the same way as you would with any other personal data you are collecting and using.

2. ## Risk to individuals

   Wherever facts or opinion exist about an identified or identifiable living person you must adhere to the Law to ensure you are taking care of that information appropriately so that their 'significant interests'[2] are not placed at risk. Any legitimate data collection made as part of your 'environmental' and 'governance' reporting requirements is unlikely to pose a high risk to individuals.

---

[1] **Pseudonymisation** "means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, where that additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable individual". Section 111, *The Data Protection (Bailiwick of Guernsey) Law, 2017*.

[2] A person's '**significant interests'** are defined in the Law as (a) any rights or freedoms conferred by law on the individual, (b) the existence or extent of a duty imposed by law on the individual, or (c) any other interests of the individual that can reasonably be regarded as significant under the circumstances.

However, covering 'social' factors could pose a risk to individuals, as (depending on what factor you are reporting on, and how you go about measuring it) you may be asking people to reveal protected characteristics about themselves. Many of the characteristics you might be asking people about - such as their sex life, gender identity, health status - are classed as 'special category data' under the Law. This type of information about people requires more safeguards under the Law because of its sensitivity. If you are collecting personal data or special category data you must take full account of the Law's requirements, as well as adhering to relevant discrimination legislation.

In all cases you can minimise the risk to individuals if you collect the relevant information anonymously. If you are linking any type of data to individuals, you must adhere to the Law's requirements to ensure you are minimising any risks that may arise.

3. **Public disclosure of data**
   ESG reporting requirements usually result in organisations publishing high-level information summaries as opposed to detailed information linked to named people. So even if you have chosen to collect information that you can link to individuals (for example: so you can check that everyone in your organisation has responded) there is no requirement for you to make that level of detail available publicly.

The seven data protection principles

Data protection is people protection. The Law seeks to protect individual's rights over information about them. The Law is built around seven common sense principles that apply whenever organisations work with information about people. To ensure effective ESG reporting while adhering to the Law's seven principles, please consider the guidelines below (remember, you can disregard this if you are collecting data anonymously):

- **Accountability**
  This is the fundamental principle that the remaining six principles rest upon. To comply with the accountability principle you must be able to **demonstrate that you take responsibility** for complying with all data protection principles. This goes to the heart of your organisation and, as such, there must be clear and demonstrable commitment from the highest level of your organisation to support the work that is needed to comply with this principle. You must be transparent about the data collection and processing practices used for ESG reporting, and provide individuals with clear information on their rights regarding their personal data.

- **Lawful, fair and transparent processing**
  There are three aspects to this principle. The first is that you must have a 'lawful processing condition' you can rely on to process any personal data as part of ESG reporting. Secondly, to satisfy the 'fairness' aspect of this principle, you must ensure that you collect data without deceiving people. And thirdly, to cover the 'transparency' aspect, you must inform individuals about the purpose, scope, and handling of their data.

- **Purpose limitation**
  To adhere to this principle, you must clearly define the purpose of collecting and processing personal data for ESG reporting. The data you collect can only be used for this specific purpose and not for any other unrelated activities.

- **Data minimisation**
  This principle dictates that you must collect and process **only the necessary** personal data required for ESG reporting. Do not gather excessive or irrelevant information. Consider whether the size of your organisation makes it possible to collect the data you need anonymously, or whether you can retrospectively anonymise the information you have already collected. Remember also, from an environmental perspective, that the less data you collect and store the less energy you will consume processing and storing it.

- **Accuracy**
  Under this principle you must ensure the accuracy and integrity of the data collected. Implement measures to regularly **update, and maintain** the quality of, the data.

- **Storage limitation**
  This principle means that you must retain personal data for the **minimum amount of time necessary** to fulfil the purpose of ESG reporting. Establish and adhere to appropriate data retention policies (the Law does not prescribe specific retention periods, so you are free to define your own as required) and securely dispose of personal data when no longer needed.

- **Security**
  To comply with this principle you must implement appropriate technical and organisational measures (e.g. restrict access to authorised personnel, maintain robust data security protocols) to protect personal data from unauthorised access, loss, or damage. Remember that special category data requires a higher degree of protection.

Additionally, consider the following best practices:

- Train managers and employees on data protection, emphasising the importance of handling individuals' personal information responsibly and securely. To raise awareness of the importance of this, you may wish to make use of the stories contained in Project Bijou.
- Document policies and procedures related to ESG reporting and data protection, making them easily accessible to stakeholders and staff.
- Consider whether it is necessary to conduct a Data Protection Impact Assessment to identify and mitigate potential risks to individuals' rights when processing their personal data for ESG reporting.

- Implement strong data governance practices, including regular audits and reviews of data processing activities, to ensure ongoing compliance with data protection law.
- Regularly review and update your ESG reporting and data protection practices to stay aligned with evolving legal requirements and industry standards.

Help and advice

If after reading the above guidance you need further clarification on your specific circumstances, please visit the Contact Us page of our website for details of our free drop-ins, and our contact information.