10 handy tips to ensure ongoing GDPR compliance

V1.0 – 06/05/2020

Disclaimer: All points covered in this presentation are the IP of Green Robin Solutions Ltd and are intended as discussion / thought points.

GREEN ROBIN SOLUTIONS

Have good data governance

- GDPR requires businesses to know what data they have on whom and why
- Good data governance, doesn’t just cover customers.
- Data should be organised where it covers:
  - Suppliers
  - Staff
  - Customers

Ensure data security

- Holding data and keeping it secure, requires a number of elements

- Data held in softcopy form:
  - Password protection
  - Storage in the Cloud
  - Use and kept up-to-date Anti-virus software

- Should a data leak, hack or loss occur. It should be possible to wipe the data

- Data held in hardcopy form:
  - Kept locked away when not in use
  - Potentially kept in a secure storage box (fireproof)

- Within your data policy, there should be a record of the safety measures taken, and training provided to staff (ongoing and for new joiners). This will help in the event of an ICO investigation

Clean data is good data

- Data cleansing should have been carried out before GDPR went live

- Have processes defined, written-down and used in regular intervals (bi-annual or annual) for data review and cleansing should be established (not just ad hoc erasure requests)

- Remember under GDPR, businesses cannot hold onto data, if it is not known what it will be used for

(Fair) Processing notice policy

- For businesses established before GDPR went live, this this document should already be in place.

- However, as a public document, it outlines what data is taken and how this data will be used

- It should provide answers to the below questions:
  - What information is being collected?
  - Who is collecting it?
  - How is the information being collected?
  - Why is it being collected?
  - How will it be used?
  - Who (if anyone) will it be shared with?

- Internally, the questions below should also be considered:
  - What will the effect on the Data Subject be?
  - Is the intended use likely to cause complaints or objections?

Personal data retrieval

- Processes should be defined, documented and regularly reviewed for dealing with personal data retrieval requests

- Under GDPR, providing the outcome of a personal data retrieval request should be:
  - Completed within 1 month
  - Provided free of charge

- Remember, under the regulation, a business is not required to provide full copies of documents / artifacts / system extracts with the data subject is mentioned. A summary such as an excel document with the list of document titles or system names where the data subject is present is sufficient

- Should a business provide copies of documents, or artifacts or system extracts. Appropriate procedures and checks should be in place to ensure that personal data of other data subjects are not also revealed.

Dealing with erasures requests

- Similar to data retrieval requests or on the back of such a request. An erasure (deletion) request may be received from a data subject

- Upon receipt of an erasure request, an acknowledgement of receipt should be sent to the data subject, outlining the steps and timelines

- Appropriate processes and checks should be established (if not already done so) to ensure the request is carried out effectively

- **Note**: GDPR is not the supreme regulation, other regulations such as anti-money laundering regulations or HMRC requirements mean that **not** all data can or should be deleted

GREEN ROBIN SOLUTIONS

Processing an erasures requests

- Similar to data retrieval requests or on the back of such a request. An erasure (deletion) / ‘right to be forgotten’ request may be received (either in writing or verbal) from a data subject

- Upon receipt of an erasure request, an acknowledgement of receipt should be sent to the data subject, outlining the steps and timelines

- Under the regulation a business has 1 month to respond to such a request

- Appropriate processes and checks should be established (if not already done so) to ensure the request is carried out effectively

- Checklist:
  - We know how to recognize a request for erasure, and we understand when the right applies
  - We have a policy for how to record requests which are received verbally
  - We understand when we can refuse a request and are aware of the information, we need to provide to the data subjects when we do so

‘Opt-in’ rather than ‘opt-out’

- Prior to GDPR businesses could record data as a default (e.g. pre-ticked boxes) this was known as ‘opt-out’
- To ‘opt-out’ a person had to take an action to actively stop an action from occurring
- Since GDPR came into effect, customers mush actively ‘opt-in’
- For example. Should a business wish to collect data for the purposes of marketing. Customers or potential customers must provide their approval for their details to be included in marketing campaigns
- Single ‘Opt-in’
  - This may be a tickbox on a website ‘yes, I want to receive XYZ’
- Double ‘Opt-in’
  - Once the customer presses ‘submit’ on a website, an automated email is sent to them with ab embedded button which generates a confirmation statement

Reporting misuse of data

- GDRP has empowered us all to appreciate the importance of our data
- Should a business owner feel that their data is being misused by a 3rd party. The below steps should be taken:
  - Contact the relevant 3rd party, outlining your concern that your data is being misused
  - If you are unhappy with the response, then the ICO should be contacted

Reporting data breaches to the ICO

- The view of the Information Commissioner's Office (ICO) is that data breaches should not happen, but if they do, then be honest about them occurring

- Regulators across all industries take a very dim view of businesses attempting to conceal when data breaches have occurred