

## Privacy and Data Protection

We're trusted with lots of personal data about our customers, colleagues, shareholders and suppliers. So it's really important we take our responsibilities seriously. Part of that involves making sure that information about how we look after people's personal data is readily available.

### Keeping us on the right track

Our Data Protection Officer (DPO) and the DPO team help us understand data protection laws and how to follow them. They make sure we're up to date and are complying with laws like the UK General Data Protection Regulation (UK-GDPR), the Data Protection Act 2018, and the Privacy & Electronic Communications Regulations 2003 (PECR). They also maintain our Privacy and Data Protection Policy Standard.

### The Standards we uphold

To ensure all our colleagues understand their responsibilities around personal data, we have what we call Standards.

These are supported by Group-wide Policy Breach & Exemption Guidance, and apply to the entire Virgin Money Group. That includes our employees, contractors, agency workers, and directors. To help colleagues stay up-to-date, all must complete data protection, data privacy and data management training at least once a year. Plus there's extra training for colleagues who handle customer data more frequently.

Our Privacy and Data Protection Policy Standard outlines our key principles. Here's a summary:

- We only process personal data when allowed to by law. When that happens, we process it in a fair and clear way and obtain consent if we need it.
- We only collect personal data for specified, explicit, and legitimate purposes set out in our privacy notice – and we won't make further use of that data for other reasons. If we need to collect personal data for new purposes, we make this clear on our website.
- We only hold personal data that's necessary for the reason we need it.
- We keep personal data accurate and up-to-date. If it's not, we delete or update it promptly.
- We delete or anonymise personal data as soon as it's no longer necessary for us to hold it.
- We make sure personal data is protected from unauthorised or unlawful use, and from accidental loss, destruction, or damage.
- We won't send personal data to another country without protecting it first.
- We encourage people to exercise all of their rights in relation to their personal data.
- We make sure our contracts with third parties include terms and conditions to protect personal data.

Continued overleaf...

- We apply privacy by default and carry out Privacy Impact Assessments to maintain our standards.
- We make sure colleagues know how to identify a personal data breach, and how to escalate it. This means that when we need to, we can tell the Information Commissioner's Office about the breach within 72 hours. If necessary, we'll also notify the person whose data was breached. In the case of a serious data breach, the Group operates an incident management process to resolve the issue and minimise the impacts.

We regularly test key privacy processes such as rights requests, breach identification, and privacy impact assessments, to make sure they're working properly. We also check that colleagues understand privacy risks associated with our business model, and that sufficient controls are in place to reduce those risks. To help us, we collect management information about key privacy processes and complaints.

As we hold lots of personal data, it's really important that everyone within Virgin Money knows who is responsible for what. Our Standards help with this knowledge, and enable colleagues to demonstrate how they are meeting those Standards.

Our Board Risk Committee is responsible for reviewing how we look after personal data. They do this in two ways:

1. Each year, a Data Protection and Privacy Report is submitted to the Board Risk Committee.
2. Throughout the year, any issues are included in the Group Chief Risk Officer's report, which is shared with the Board Risk Committee.

In addition, a Privacy Forum and Enterprise Data Committee operate in the first line of defence to help identify, discuss and manage data issues (including data quality and data privacy issues).

## Privacy Notice

You can find out lots more about how we collect, use, share and store personal data in our Privacy Notice. We've also got details about data protection rights in there too.

## Who can I ask for more info?

You can email our DPO at [CYBG.data.protection.officer.queries@cybg.com](mailto:CYBG.data.protection.officer.queries@cybg.com) or write to them at Group Data Protection Officer, Group Risk, Level 3, 51 West George Street, Glasgow G2 2JJ.