Appendix 1 Data Breach Register Template

The CFO responsible for keeping this register up to date.

Date of breach	Outline of facts	Effect of the breach	Remedial action taken	Regulatory bodies informed if any e.g. ICO	Data Subjects informed, if required

Appendix 2 Risk Assessment of the Data Breach

	Question	**Response**
1.	Precisely what data has been (or is thought to have been) lost, damaged or compromised?	
2.	Is any of the data special category personal data as defined by the GDPR? This would be: i. Racial or ethnic origin ii. Political opinions iii. Religious or philosophical beliefs iv. Trade union membership / activities v. Medical data (both physical and mental health related) vi. Sexual orientation and data concerning a person's sex life vii. Genetic and biometric data viii. Criminal records, administrative judgements or sanctions, and details of alleged offences. If any of these types of data are involved this makes the breach more serious.	
3.	Who are the affected individuals e.g. employees, customers, third parties?	

4.	How many individuals have definitely been affected and how many potentially affected in a worst case scenario?	
5.	What harm might be caused to individuals (not Chargifi)? The individuals do not necessarily need to be those whose personal data was involved in the breach. Harm should be interpreted broadly, for example to include: (a) distress; (b) discrimination; (c) loss of confidentiality; (d) financial damage; (e) identity theft; (f) physical harm; and (g) reputational damage.	
6.	What harm might be caused to the Chargifi? For example, reputational damage and financial loss.	
7.	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point.	

	(a) Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen? (b) Were any technical protections in place e.g. was the data protected by encryption? (c) Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? (d) Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?	