HSBC Top 10 Treasury Checklist

Data

What data do you hold that is covered under GDPR – e.g. beneficiary information, employee information etc.? Remember that any information that could identify a person, e.g. email addresses are within the scope of the regulation.

Consent

Have you confirmed the processing condition you are relying on to process personal data? Where consent is required, do you have consent to process the data, are any existing consents compliant with GDPR requirements, and do those consents cover the processing you are intending to carry out? Where you're not relying on consent, have you confirmed your documentation does not suggest otherwise?

Responsible person

Where you are required to appoint a data protection officer (DPO), do you know who this is and has s/he scrutinised your systems and processes?

Data management

Have you incorporated data subject rights, such as the 'right to be forgotten' in the way that you hold your data? Do you have processes for receiving and dealing with requests from individuals, including identifying when these rights apply, and can you achieve them if required?

Storage

Where is your data held? Onsite/offsite/cloud? In-house/outsourced?

Third parties

What assurances do you have of GDPR compliance by third party processors? Have you ensured your contracts reflect GDPR requirements? Ensure you identify and classify data, capture these in your record of processing, and understand the rules about data held by others outside your organisation.

Encryption

The GDPR encourages use of data security measures such as encryption – is your data encrypted? If not, does your TMS/ERP vendor have a new version available to which you to which you can upgrade, or do you need to introduce new technology?

Threats

Are your staff aware of phishing risks and other potential cyberthreats? Does this also apply to remote users/business units?

Breaches

Do you have a process for reporting of breaches, and have you tested it?

Audit

Are your prevention/detection tools auditable in case of a regulatory request or GDPR investigation?