

Data Privacy and Corona

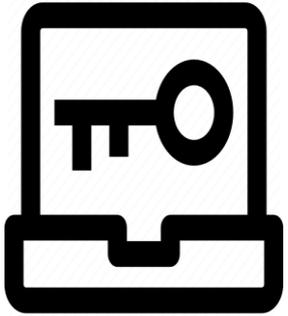


Tips to comply with GDPR
during the pandemic

Kersi F. Porbunderwalla
Hernan Huwyler

The logo for the EU GDPR Institute, featuring the letters 'EU' in a blue box with yellow stars, followed by 'GDPR INSTITUTE' in a white box with blue text.

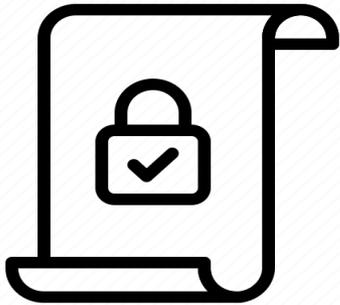
The logo for Copenhagen Compliance, featuring the words 'COPENHAGEN' and 'COMPLIANCE' in white text on a blue background.



Review changes in user access to ERP, CRM and shared folders

- ✎ As of today and during the response plans**
- ✎ Cover IT admins, employees and consultants**
- ✎ Focus on display and edit large databases**
- ✎ Update the segregation of duties**
- ✎ Recertify users with process owners**

Reprioritize tasks



Regulators understand that resources were diverted during a pandemic

- ✎ Inform extended periods to new and backlogged subject access requestors**
- ✎ Delay plans for audits to processors**
- ✎ Focus on contracts with new vendors and services engaged during the response actions**

Increase security controls



Homeworking poses higher human error and fraud risks

- ✎ Ask IT for updating the remote VPNs and access solutions**
- ✎ Assess security practices in video conferences**
- ✎ Check for failed logins to critical systems**
- ✎ Review changes in privacy and security settings**



Response actions significantly changed the data processing

- ✎ Update and review the RoPA for new cloud and personal storage databases and end-user applications created for teleworking**
- ✎ Review the adjustment of the scope of the data loss prevention to the changes in the IT assets**
- ✎ Assess the need for updating DPIAs**



Coronavirus is a catalyst for cybercrime

- ✎ Investigate for missing assets during the response activities**
- ✎ Ensure the review of security logs during the crisis**
- ✎ Request updates to data processors**