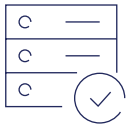
Data breach response plan



The first 48–72 hours after finding out about the data breach are of critical importance. Use this action plan and act swiftly.

Action plan for a data breach	Yes	No	Notes
Document the time and way of detecting the breach, who detected it and when the breach occurred.			
Notify the responsible team member and the IT specialist and if necessary, involve cybersecurity experts independent from third parties.			
Eliminate the existing vulnerability of the data system while maintaining all the logs and other evidence related to the breach.			
If the breach continues, isolate all the affected systems by disconnecting them from the network, while maintaining the logs and documenting all the activity.			
Check whether other systems are unaffected by the breach.			
Document the amount, sensitivity and nature of data that was breached and the period of the breach.			
If necessary, consult a third party counsel and inform the relevant authorities of the data breach.			
If necessary, consult a third party counsel and communicate to the data subjects affected if required by law.			
Identify the cause for data breach and ensure the future security of the systems.			