Employee Data Privacy – India

Breach Notification

Are there any data breach notification requirements?

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Local data protection regulations have required data controllers to report such breaches in certain circumstances.

Companies and individuals are mandated to report specific types of cyber security incidents to the Indian Computer Emergency Response Team (CERT-In) as soon as possible under the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013. These include:

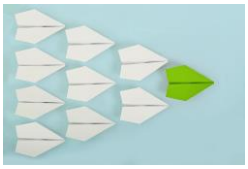
- targeted scanning or probing of critical systems/networks
- compromise of critical systems and information
- unauthorized access of IT systems and data
- defacement of a website or intrusion into a website and unauthorized changes
- malicious code attacks
- attacks on servers and network devices
- identity theft, spoofing, phishing attacks
- Denial of Service and Distributed Denial of Service attacks
- attacks on critical infrastructure, SCADA systems and wireless networks
- attacks on applications (e-governance, e-commerce, etc.)

Per directions issued by the CERT-In (“Directions”) dated April 28, 2022, all service providers, intermediaries, data centers, body corporates, and government organizations, must report cyber incidents to the CERT-In within six hours of becoming aware of an incident. The list of cyber incidents which must be mandatorily reported include:

- targeted scanning/probing of critical systems/networks;
- the compromise of critical systems/information;
- unauthorized access of IT systems/data;
- defacement of a website or intrusion into a website and unauthorized changes (ex., inserting links to external websites);
- malicious code attacks;
- attacks on servers;
- identity theft, spoofing, and phishing attacks;
- Denial of Service and Distributed Denial of Service attacks;

- attacks on critical infrastructure, SCADA systems and operational technology systems and wireless networks;
- attacks on applications such as e-governance, e-commerce, etc.;
- data breaches;
- data leaks;
- attacks/incidents affecting digital payment systems;
- attacks through malicious mobile Apps;
- fake mobile Apps;
- unauthorized access to social media accounts;
- attacks or malicious/suspicious activities affecting cloud computing systems/servers/software applications;
- attacks or malicious/suspicious activities affecting systems/servers/ networks/ software/applications related to Big Data, blockchain, virtual assets, virtual asset exchanges, custodian wallets, robotics, 3D and 4D printing, additive manufacturing, drones; and,
- attacks or malicious/suspicious activities affecting systems/servers/software/ applications related to artificial intelligence and machine learning.

In addition to these reporting obligations, CERT-In can request information and give direction to entities relating to cybersecurity (with potential penalties including jail time for noncompliance) (The Information Technology Act, 2000 and its amendments).



HR Best Practices:

Make sure to follow any security and data protection controls outlined in your company's security policies (this includes regular audits by independent agencies). In the event of a possible cybersecurity incident, reach out to the Indian Computer Emergency Response Team as soon as possible.

Last updated July 2022.