Employee Data Privacy – Brazil

Fines and Penalties

What are the penalties for noncompliance with any applicable data protection laws?

Noncompliance with Data Privacy Laws and Data breaches may lead to sanctions, fines, and penalties. The amounts are usually calculated according to the risk to which personal rights were exposed and the preventive measures taken by the data controllers, processors and sub-processors in relation to their respective role in the chain of personal data processing.

Brazil's Federal Constitution gives individuals the right to compensation for economic and non-financial damages relating to privacy violations.

Denying an individual's right to personal data access, correction and removal under the Consumer Protection Code (which applies to consumers) could result in a fine, compensation (for the individual whose right was violated) and/or up to one year of imprisonment.

Violating the Internet Law can result in sanctions, including:

- warnings;
- suspension and/or prohibition of data processing; and,
- a fine of up to 10% of annual revenues in Brazil.

Cybercrimes, including breaking into third-party systems to obtain or destroy information can result in a fine and imprisonment (Law 12,737/2012).

New General Data Protection Law

Administrative fines and penalties may be imposed if there is a violation of the General Data Protection Law (LGPD). Penalties include:

- warnings with deadlines for corrective measures;
- fines of up to 2% of annual revenue in Brazil (based on the previous financial year) up to a maximum of 50 million reais per violation;
- daily fines up to the same limit;
- public disclosure of the violation;
- blocking the personal data relating to the infraction, until corrected; and,
- deleting personal data relating to the infraction.

In addition, the below penalties may be imposed in recurring cases, after at least one of the sanctions above has already been imposed for the same reason, and if employers (or other

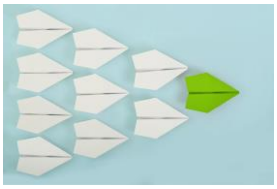
controllers) are being sanctioned by other authorities:

- partially suspending the operating database in which the infraction occurred for up to 6 months, and extendable until the employer (or other controller) implements compliant processing operations;
- suspending the personal data processing in which the infraction occurred for up to 6 months, and extendable for the same period; and,
- partially or fully banning data processing activities.

Sanctions will be based on:

- the severity and nature of the violation and its impact on individuals' rights;
- the good faith of the offender;
- how the offender benefited or hoped to benefit from the violation;
- the economic circumstances of the offender;
- whether this is a repeat offense;
- damages;
- the cooperation of the violator;
- repeated and clear adoption of measures to reverse or mitigate the impact of the incident;
- adoption of good practices and policies;
- prompt adoption of corrective measures; and,
- what's proportionally appropriate given the nature of the breach.

The penalties under the LGPD are cumulative to other applicable penalties. Note that employees can sue employers for "moral damages" for mishandling personal data.



HR Best Practices:

Before processing employees' personal data, make sure to be in line with the security measures necessary to ensure data security within your organization. Furthermore, ensure all data processors have data breach response plans in place.

Last updated November 2022.