pepeliaev group

The law has come into effect to introduce criminal liability for personal data leakages

FAO personal data operators

Pepeliaev Group advises that, on 11 December 2024, Federal Law No. 421-FZ "On amending the Criminal Code of the Russian Federation" dated 30 November 2024 (the "Law") came into force.

The Law supplements the Russian Criminal Code (the 'Criminal Code") with article 272.1, which provides for a criminal penalty for computerised information that contains personal data being illegally used, and/or transmitted and gathered, and/or stored. The penalty will also apply to information resources being created and/or operated which are designed for such information to be illegally stored and/or disseminated.

To whom will criminal liability apply? Will it extend to a company's employees?

The grounds for criminal liability include the commission of an act that contains all of the elements of a crime provided for in the Criminal Code.

Consequently, criminal liability will apply to a person who has committed specific acts. These include: the illegal use, transfer (dissemination, provision of or granting access to), collection and storage of computerised information that contains personal data which has been obtained through unlawfully accessing tools for processing and storing information or otherwise interfering with such tools being operated or through any other illegal methods.

As far as employees of companies are concerned, part 3 of the article in question provides for a separate body of a crime, i.e. committing the crime through an abuse of one's official position, with a higher fine and longer term of imprisonment being stipulated for this body of the crime.

Can a company's CEO/DPO be held criminally liable?

According to the general principles of criminal law, a person is subject to criminal liability only for those publicly dangerous acts (omissions), as well as the consequences posing a danger to the public of such actions, with respect to which their fault has been established. No-fault liability, i.e. criminal liability for inflicting damage without any fault, is not permitted.

A company's management/data protection officer (DPO) may have criminal liability imposed if their actions contain elements of the crime and their fault has been ascertained.

As a counter-example, we can take article 143 of the Criminal Code ("Violating occupational safety requirements") which provides for criminal liability for requirements for occupational safety being violated by a person who is obliged to comply with such requirements, provided that this has resulted in severe harm to the health of, or even in the death of, a person through such negligence. In this case, the person will be held liable because of certain obligations being imposed on them (it is not enough for the obligations to be imposed - the requirements must have been violated, which has resulted in harm being caused).

One should not forget about the concept of complicity in a crime which is understood to mean the deliberate joint participation of two or more persons in the perpetration of a deliberate crime. In addition to the actual perpetrator of a crime, other parties to the crime include: the organiser of a crime, an instigator of the commission of a crime and an accomplice. Whether participants in a crime are liable is determined by the nature and degree of their respective participation in the perpetration of the crime.

A perpetrator is a person who has actually committed the crime or who was directly involved in the crime being committed together with other persons (joint participants in the crime). An organiser of a crime is a person who has arranged for, and overseen, the commission of the crime. An instigator means a person who has induced another person to commit the crime by persuading, bribing, threatening or otherwise influencing such other person. An accomplice is a person who aided the commission of the crime by providing advice, instructions, information, tools or means for committing the crime or by alleviating obstacles. This is also a person who has promised in advance to hide the criminal or the tools and means by which the crime was committed, as well as the traces of the crime or items which were obtained in an illegal way, and who has also promised in advance to purchase or sell such items.

Will criminal liability be extended to computer hackers?

The range of persons to whom article 272.1 of the Criminal Code applies is not limited. It applies to any offenders who illegally collect, store, use or transfer computerised information that contains personal data. This means that the article equally applies to cybercriminals and computer hackers.

In addition, computer hackers can face criminal liability under, among other provisions, articles 272 ("Unlawfully accessing computerised information"), 273 ("Creating, using and distributing malicious computer programs"), 274.1 ("Unlawfully interfering with critical information infrastructure of the Russian Federation"), 183 ("Illegally obtaining and disclosing information that constitutes commercial, tax or banking secrets") and 159 ("Fraud") of the Criminal Code.

Conclusions

1. Criminal liability will apply to a person who has committed specific acts. These include: the illegal use, transfer (dissemination, provision of or granting access to), collection and storage of computerised information that contains personal data which has been obtained through unlawfully accessing tools for processing and storing it, or otherwise interfering with how such tools are operated or through any other illegal methods.

2. A higher fine and longer imprisonment have been stipulated for cases when an officer of a company commits such actions while abusing their official position.

3. The company's management/DPO may have criminal liability imposed on general grounds (provided that their actions contain elements of the crime and their fault has also been ascertained) rather than owing to their office. This is in contrast to liability, for instance, under article 143 of the Criminal Code ("Violating occupational safety requirements"). One should not forget about the concept of complicity in crime.

What to think about and what to do

- An audit should be conducted into how personal data is processed and all processes should be identified within the scope of which personal data is transferred. Any excessive processing of personal data (including the transfer thereof) should be excluded. It should be ensured that personal data is processed (including the transfer thereof) in compliance with the legal requirements.
- Legal, organisational and technical measures should be determined that are necessary to safeguard personal data from being accessed unlawfully or accidentally, from being destroyed, modified, blocked, copied, provided or distributed, as well as from other unlawful actions with respect to personal data. It should be ensured that all necessary measures are taken.
- A full set of local regulations should be developed to regulate the processing and safeguarding of personal data.
- Orders for/agreements with third parties should be formalised for personal data to be processed.
- Training events in the field of personal data should be held regularly for the company's employees as a measure that is effective in preventing any data leakage.

Help from your adviser

The lawyers of Pepeliaev Group stand ready to provide comprehensive legal support to companies.

Our firm offers the following range of services:

1. Providing support to clients in cases of leakages of personal data on a round-the-clock basis;

2. Drafting notifications to the communications regulator Roskomnadzor;

3. Devising and holding training in the field of personal data for the client's employees;

4. Providing one-time consultations on any issues associated with the processing of personal data;

5. DPO - providing legal support with regard to personal data processing on a subscription basis at favourable rates;

6. Conducting an audit of personal data processing;

7. Devising a roadmap to bring a client's activity in line with the requirements of the legislation on personal data;

8. Devising a full set of internal regulations to regulate the processing and protection of personal data;

9. Advising on issues of personal data processing within the scope of interactions with third parties (including drafting all necessary documents).

Contact details

Nikolay Solodovnikov
Partner

Tel.: +7 (495) 767 00 07
n.solodovnikov@pgplaw.ru

Polina Bardina
Head of Digital Group

Tel.: +7 (495) 767 00 07
p.bardina@pgplaw.ru

Nataliya Balekina
Associate

Tel.: +7 (495) 767 00 07
n.balekina@pgplaw.ru