Crowe

ACA IT-Solutions, onderdeel van Crowe

Whitepaper:

GDPR

Are you prepared for new European privacy legislation?

ACA IT-Solutions, onderdeel van Crowe

GDPR

The new European privacy act requires thorough preparation

Automation and digitisation are making life and doing business a lot easier. Technological developments are taking place in rapid succession. In addition to being convenient, these developments involve risks as well, for example in terms of security and privacy. It regularly happens that personal data of customers or employees are wrongly made public or end up in the wrong hands.

The protection of sensitive data is an important issue for the Dutch government and the European Union. For that reason, the Personal Data Protection Act (PDPA) will be replaced by a more comprehensive European variant that is tailored to the digital era. This legislation is known as the General Data Protection Regulation (GDPR) and is currently already in force. As of 25 May 2018 it will also be actively enforced by the Dutch Data Protection Authority (Dutch DPA). This means that all organisations collecting, editing or processing personal data must be GDPR-compliant as of that date. For that reason, organisations and their employees must make thorough preparations.

AUTORITEIT PERSOONSGEGEVENS

> *The GDPR legislation is an important guideline for organizations.*
>
> Maarten de Rooij, IT Business Professional ACA IT-Solutions

GDPR compliance becomes vital for every organisation

The new privacy legislation was created in order to arrive at better protection of personal data of individuals within the EU and to harmonise agreements in this respect. This way, European citizens can be sure that their data is handled and protected in the same way in all EU member states. This will affect the way in which personal data must be documented for virtually all bodies and companies. The definition of what exactly personal data is has been expanded and specified in the GDPR as well. Partly due to this broadening of the term ‘personal data’, virtually every organisation has privacy sensitive information at its disposal that falls under the GDPR. This includes customer data (including business e-mail addresses) copies of ID cards, credit card and/or bank details, employee’s details etc. In order to ensure that this information is stored, used and managed properly, the GDPR has dozens of guidelines and regulations.

ACA IT-Solutions, onderdeel van Crowe

The GDPR measures are compulsory

Complying with the GDPR and taking measures is strictly compulsory. As the lack of a sound privacy policy increases the likelihood of data breaches. The Dutch DPA can severely penalise data breaches resulting from negligence. The sanctions range from warnings and binding measures to a maximum penalty of 20 million euro or 4% of the global annual turnover. This can exceed a company's capacity and result in bankruptcy.

However, this is not the only reason to ensure that the organisation complies with the privacy regulations. A data breach and a poor policy can result in severe reputational damage. In certain cases, the Dutch DPA will publicly announce incidents, especially if data breaches occur more often at an organisation. The parties affected by a data breach must be informed, which might result in negative media attention.

Basic principles of the GDPR

The General Data Protection Regulation (GDPR) in Dutch is referred to as the AVG ('Algemene Verordering Gegevensbescherming'). In principle, there are various basic principles that apply to any organisation:

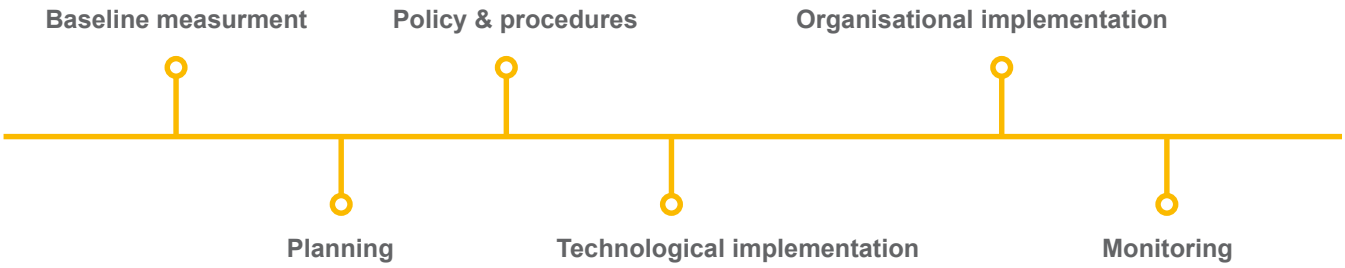
- ***Lawfulness, fairness and transparency*** – Personal data must be processed in a lawful, fair and transparent manner in relation to data subjects.
- ***Integrity and confidentiality*** – Appropriate security of personal data must be ensured, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- ***Data minimisation*** – The storage and use of data must be limited to data that is necessary and exclusively available to employees that require the relevant data for business purposes.
- ***Purpose limitation*** – Personal data may only be used for explicit and legitimate purposes.
- ***Storage delimitation*** – Personal data will not be kept longer than necessary.

ACA IT-Solutions, onderdeel van Crowe

The solution: realise, execute and monitor security policy

The new act will have an enormous impact on the way organisations work and act. In summary, ‘appropriate technical and organisational measures’ must be taken to protect privacy, which involves a lot of work. The solution for a sound privacy policy is threefold:

1. A good security of the ICT environment. The ICT Security of your business environment must be structured in such a way that risks are avoided.
2. Organisations are expected to prepare policies and procedures. In addition, documents must be drafted that record arrangements with third parties (processing agreements).
3. Following up policy and procedures. This requires organisational adjustments. All employees must be aware of the dos and don’ts and act accordingly.



The comprehensive approach of ACA IT-Solutions

To ensure that your organisation is fully GDPR-compliant, various technical and organisational steps are required. ACA IT-Solutions employs specialists who will guide you through the entire process, both in terms of execution, advice and policy. We will take you through all the steps in the process of becoming, and remaining, GDPR-compliant. We will support you in drafting policy and procedures. Moreover, we will help you create involvement and awareness on the part of your employees.

In addition to the organisational facets, securing the ICT environment is also an important factor. We will also be able to perfectly support you from a technical point of view. We have over 30 years’ experience with advice, design, installation, system administration and support (24x7) of ICT environments. This makes ACA IT-Solutions a reliable partner for many different types of organisations, from SME to Enterprise.

Advice & support

Contact

Would you like more information or are you interested in an appointment? Please contact us.

Address

ACA IT-Solutions, onderdeel van Crowe
Beukenlaan 40-50
5651 CD Eindhoven

Contact

040 - 8 800 100
info@aca-it.nl
www.aca-it.nl

ACA IT-Solutions, onderdeel van Crowe

How privacy proof is your organisation?

Use the checklist below and check whether your organisation's ICT policy complies with the privacy legislation. This checklist can provides assistance and gives an indication of the requirements.

Are the following obligatory subjects arranged for?

Have all employees received privacy regulations? . . . . . YES NO

Is there an action plan for all employees in the event of a data leak? . . . . . YES NO

Is it known who has access to sensitive personal data? . . . . . YES NO

Is privacy sensitive information stored outside of the organisation without knowledge . . . . . YES NO

Is there a responsible party in terms of use of social media by employees? . . . . . YES NO

Does your security officer have set of regulations for internal privacy and ICT management? . . . . . YES NO

Has consent been given for storing personal data of customers? . . . . . YES NO

Has consent been given for the publication of photographs of employees? . . . . . YES NO

Have all employees been informed about the applicable Personal Data Protection Act? . . . . . YES NO

Is privacy sensitive data that is not necessary for the organisation removed in a timely manner? . . . . . YES NO

Do employees have access to a step-by-step plan regarding the execution of the privacy policy? . . . . . YES NO

Is there a protocol for the reporting, registration and processing of security incidents? . . . . . YES NO

Is privacy protection ensured when an employee leaves the organisation? . . . . . YES NO

Has a processing agreement been sent to all external processors? . . . . . YES NO

Has it been determined who has access to privacy-sensitive information (internal and external)? . . . . . YES NO

Has the notification number of the Dutch Data Protection Authority been included in the records? . . . . . YES NO

Do all external processors comply with the criteria of the privacy legislation? . . . . . YES NO

Are all external processors insured against liability in case of any data breaches? . . . . . YES NO

Have the correct legal steps been followed for the implementation of the ICT usage policy? . . . . . YES NO

Do the employees have access to sound ICT user regulations? . . . . . YES NO

Do the personal devices of the employees (mobiles, laptops)

comply with the ICT Security requirements? . . . . . YES NO

Is it verified whether employees do not have any illegal software on their own devices (BYOD)? . . . . . YES NO

Is there an overview of the technical measures that have been taken? . . . . . YES NO

Have the preventive measures been brought to the attention of the employees? . . . . . YES NO

Have you answered 'no' to more than one question, or do you have any doubts about your answers?

Do not take any risks and do not hesitate to contact us. We are happy to come by your office to discuss your situation without any obligations.