



# Data Protection Policy

The General Data Protection Regulation (GDPR) 2018 regulates the collection, use, disclosure and processing of personal information of individuals in the EU. It replaces existing European legislation, such as Data Protection Directive (officially Directive 95/46/EC), and introduces new requirements, it alters existing concepts, which means that businesses will need to review their existing processes to make sure they are compliant.

Private investigative businesses and services they provide (be that plain investigations, background checks, due diligence, insurance claims, etc) can involve significant personal data processing, so complete adoption of GDPR compliance is crucial. It is important for businesses to raise awareness of the changes, review current privacy notices, background screening policies and in general, their approach to this new age of data protection regulations and requirements, which GDPR 2018 certainly is.

This present DPP is valid for the services provided by Background Check Romania, a division of CIDP "Tanase V. Iulian" (trading online) as Background Check Romania).

## CONTEXT AND OVERVIEW

Replaces current policy on: **25<sup>th</sup> of May 2018**  
Approved on: **08<sup>th</sup> of May 2018**

Policy prepared by: **Julian Tanase**  
Becomes operational on: **25<sup>th</sup> of May 2018**

### INTRODUCTION

CIDP “Tanase V. Iulian” (also trading as Background Check Romania) needs to gather and use certain information about individuals and /or businesses.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards – and to comply with the law.

### WHY THIS POLICY EXISTS

This data protection policy ensures CIDP “Tanase V. Iulian” (also trading as Background Check Romania) shall:

- ✓ Comply with data protection law and follow good practice
- ✓ Protect the rights of staff, customers and partners
- ✓ Be opened on about how it stores and processes individuals’ data
- ✓ Protect itself from the risks of a data breach

### DATA PROTECTION LAW

The GDPR 2018 describes how organisations – including CIDP “Tanase V. Iulian” (also trading as Background Check Romania) – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The GDPR 2018 is underpinned by eight important principles. These say that personal data must:

- ✓ Be processed fairly and lawfully
- ✓ Be obtained only for specific, lawful purposes
- ✓ Be adequate, relevant and not excessive
- ✓ Be accurate and kept up to date
- ✓ Not be held for any longer than necessary
- ✓ Processed in accordance with the rights of data subjects
- ✓ Be protected in appropriate ways
- ✓ Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

### PEOPLE, RISKS AND RESPONSIBILITIES

#### Policy scope

This policy applies to the head office of CIDP “Tanase V. Iulian” (also trading as Background Check Romania) and also to (if existing):

- ✓ All branches of CIDP “Tanase V. Iulian” (also trading as Background Check Romania)
- ✓ All staff and volunteers of CIDP “Tanase V. Iulian” (also trading as Background Check Romania)
- ✓ All contractors, suppliers and other people working on behalf of CIDP “Tanase V. Iulian” (also trading as Background Check Romania)

It also applies to all data that the company holds relating to identifiable individuals, even if that



information technically falls outside of the GDPR 2018. This can include, but may not be limited, as follows:

- ✓ Names of individuals
- ✓ Postal addresses
- ✓ Email addresses
- ✓ Telephone numbers

## DATA PROTECTION RISKS

This policy helps to protect CIDP “Tanase V. Iulian” (also trading as Background Check Romania) from some very real data security risks, including:

1. Breaches of confidentiality. For instance, information being given out inappropriately.
2. Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
3. Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

## RESPONSIBILITIES

Everyone who works for or with CIDP “Tanase V. Iulian” (also trading as Background Check Romania) has some responsibility for ensuring data is collected, stored and handled appropriately, as follows:

- ✓ Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.
- ✓ However, these people have key areas of responsibility:
- ✓ Keeping the board updated about data protection responsibilities, risks and issues.
- ✓ Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- ✓ Arranging data protection training and advice for the people covered by this policy.
- ✓ Handling data protection questions from staff and anyone else covered by this policy.
- ✓ Dealing with requests from individuals to see the data CIDP “Tanase V. Iulian” (also trading

as Background Check Romania) holds about them (also called ‘subject access requests’).

- ✓ Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
- ✓ Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principal

## GENERAL STAFF GUIDELINES

The following are general guidelines, which are mandatory to be observed and applied as per case maybe:

- ✓ The only people able to access data covered by this policy should be those who need it for their work.
- ✓ Data should not be shared informally.
- ✓ Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- ✓ In particular, strong passwords must be used and they should never be shared.
- ✓ Personal data should not be disclosed to unauthorised people, either within the company or externally.
- ✓ Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

## DATA STORAGE



These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

- ✓ When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- ✓ These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
- ✓ When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- ✓ Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- ✓ Data printouts should be shredded and disposed of securely when no longer required.
- ✓ When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- ✓ Data should be protected by strong passwords that are changed regularly and never shared between employees.
- ✓ If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- ✓ Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- ✓ Servers containing personal data should be sited in a secure location, away from general office space.
- ✓ Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- ✓ Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- ✓ All servers and computers containing data should be protected by approved security software and a firewall.

## DATA USE

Personal data is of no value to CIDP "Tanase V. Iulian" (also trading as Background Check Romania), unless

the business can make use of it. However, it is our resolve and policy as follows:

- ✓ When personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:
- ✓ When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- ✓ Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- ✓ Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- ✓ Personal data should never be transferred outside of the European Economic Area.
- ✓ Employees should not save copies of personal data to their own computers.
- ✓ Always access and update the central copy of any data.

## DATA ACCURACY

The law requires CIDP "Tanase V. Iulian" (also trading as Background Check Romania) to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort CIDP "Tanase V. Iulian" (also trading as Background Check Romania) should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. Therefore:

- ✓ Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- ✓ Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- ✓ CIDP "Tanase V. Iulian" (also trading as Background Check Romania) will make it easy for data subjects to update the information CIDP "Tanase V. Iulian" (also trading as Background Check Romania)





holds about them. For instance, via the company website.

- ✓ Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

## SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by CIDP "Tanase V. Iulian" (also trading as Background Check Romania) are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.
- If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller / data processor at [office@backgroundcheck.ro](mailto:office@backgroundcheck.ro). The data controller may supply a standard request form, although individuals do not have to use this.

The data controller / data processor will always verify the identity of anyone making a subject access request before handing over any information.

## DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the GDPR 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CIDP "Tanase V. Iulian" (also trading as Background Check Romania) will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from a legal adviser where necessary.

## PROVIDING INFORMATION

CIDP "Tanase V. Iulian" (also trading as Background Check Romania) aims to ensure that individuals are

aware that their data is being processed, and that they understand:

- ✓ How the data is being used
- ✓ How to exercise their rights

---

For more information on our data protection policy, our GDPR Service Agreement addendum or about other additional steps implemented starting the 25<sup>th</sup> of May 2018, please contact us at:

+40-(0)-741394667

[office@backgroundcheck.ro](mailto:office@backgroundcheck.ro)

[www.backgroundcheck.ro](http://www.backgroundcheck.ro)