

## Registry Controller

Profos Executive Search Oy  
Fredrikinkatu 34 B 23  
00100 Helsinki, FINLAND

## Data Protection Officer

The Data Protection Officer is the Managing Partner of the company, Harri Hämäläinen. All inquiries regarding the registry can be sent to info (at) profos.fi.

## Name of the registry

Profos Executive Search recruitment and personal evaluation registry, including the résumés and additional materials delivered by the candidates.

## Purpose of processing personal data

Personal data is utilized during recruitment and personal evaluation assignments conducted by Profos Executive Search Ltd. By submitting their data, individuals give consent to store and to use their personal data.

Personal data is used to conduct recruitment and personal evaluations.

## Registry contents

The registry includes following personal data:

- Name
- Age
- Education
- Contact information
- Title
- Employment history
- Résumé
- Application
- Other relevant data

## Data sources of the registry

The information included in the registry is gathered from the candidates by phone calls, internet, meetings, and other similar means. In addition to the candidates, data sources include the referees as well as persons involved in the recruitment process of Profos Executive Search Ltd. The application and relevant personal data are retained for two years after being sent to Profos Executive Search or after the latest update of the data.

## Disclosure of the data

The data received from the candidate, such as the résumé and the application, can be handed over to the assignee of the recruitment or personal evaluation.

The data is not given to other parties unless ordered by the law or an order by an official degree.

## Protection of the registry

All personal data is stored with confidentiality. The data can be accessed solely by employees who have the permission to handle data due to the nature of their work. Each employee possesses their own usernames and passwords to the system.

The Data is stored in systems that are protected by firewalls, passwords and other appropriate means. The data can be accessed by preselected persons only.

## Right to access and erasure

The candidate has the right to access their stored data. The request for access and the possible request of erasure of data is to be signed and delivered in written form to controller mentioned above.