The termination of an employment agreement: What to do with data carriers containing (former) employee's private data?

Introduction

It is quite common that employees are provided with a company laptop, tablet or mobile phone by their employer. Such devices remain company property and are made available to employees in order to enable them to perform their duties. In practice, it happens that employees do not use such devices for business activities only, but also use it for private matters. In this blog, we will discuss what consequences this may have when the employment agreement is terminated.

Return of company property when the employment is terminated

When an employment agreement terminates, the employee has to return company property -such as data carriers- to the employer. If employee's private data are (still) stored on such device, parties may face a challenging situation.

Recently, a Dutch judge in summary proceedings handed a dispute between (former) employee and employer[1]. Since the employment agreement has ended, the (former) employee had to return to the employer a company laptop. The (former) employee refused to do this because the laptop still contained his private data. In order to erase such private data, the (former) employee had to get access to the company network again. This was not acceptable to the employer. The judge in summary proceedings ruled that the (former) employee had to go to the employer's IT department to have the private data 'erased' on the spot. In this way, the interests of both parties were served: the employer was not able to see any of the private data and the (former) employee did not need to get access again to the company network.

Previous case law

In Dutch case law, the concept of "*privétisering* of the workplace" is accepted, meaning that the employer cannot prohibit a certain degree of private (non-business) email and internet use during working hours. This has also been accepted in the international context (The Council of Europe, ECHR 2017).

As a result, it is possible (and likely) that an employee's private data is still on the employer's data carriers or in the employer's company's network when the employment agreement is ending.

Our approach to prevent complaints or disputes

Considering the above, parties are best served with a clear policy or regulations in this respect. Such regulations can be part of the staff handbook (personnel manual) and explain the employer's terms and conditions as to private use of e-mail and internet (including: social media) during working hours

[1] https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOVE:2022:2365

and how employer monitors compliance. The Works Council will need to be involved, if established. Also, such a policy or regulations need to indicate what applies in the off-boarding phase, when the employment agreement is (nearly) ended. For this phase clear instructions are useful, instructing employees to make sure that at the end of the employment no private data is on employer's data carriers **and at the same time** no business information is kept on employee's private devices.

At request, we can draft or amend your policy/-ies in this respect and review or amend your standard templates, for example your template 'offboarding' letter, where necessary. Please contact us at https://hplaw.nl/nl/contact/.