



Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

REGIONALES
RECHENZENTRUM

UHH · RRZ · Schlüterstraße 70 · 20146 Hamburg

To:

Universität Hamburg staff

Bernd Flickenschild

Information Security Officer

Schlüterstraße 70
20146 Hamburg

Tel: +49 40 42838-2457

Fax: +49 40 42838-6270

bernd.flickenschild@uni-hamburg.de

www.uni-hamburg.de

08.12.2020
RRZ

Deactivation of automatic work email forwarding services for Universität Hamburg staff

Dear Colleagues,

On 28 May 2018, Universität Hamburg's Executive Board decided to follow the recommendation of the Information Security Officer regarding the automatic forwarding of work emails. This is explained in greater detail in the attached memorandum.

The automatic forwarding of work emails is now prohibited for staff at Universität Hamburg and will also be prevented technically.

Over the coming weeks, the Regional Computing Center (RRZ) will systematically review all automatic forwarding set up on our central email systems and delete—and permanently prevent—this.

You will also be notified of this individually.

Sincerely,

Prof. Dr.-Ing. Stephan Olbrich

Attachment:

Memorandum: "Automatic forwarding of work emails for Universität Hamburg staff,"
Information Security Officer of Universität Hamburg, 19 March 2018



UHH · RRZ · Schlüterstraße 70 · 20146 Hamburg

CIO board via the RRZ director

Bernd Flickenschild

Information Security Officer

Schlüterstraße 70
20146 Hamburg

Tel: +49 40 42838-2457

Fax: +49 40 42838-6270

bernd.flickenschild@uni-hamburg.de

www.uni-hamburg.de

19.03.2018

Memorandum: “Automatic forwarding of work emails for staff at Universität Hamburg”

Current situation

When automatic email forwarding is used, protected data passes to a third party—here, the email provider. This third party, however, does not necessarily ensure that the required protective measures are in place. Also, Universität Hamburg has no influence over external email providers and thus has no means of monitoring and controlling introduction of the necessary technical and organizational measures. Various aspects come into play here:

Data protection

The University has a general obligation to organize its operations so that applicable laws are observed and no legal violations occur (compliance)—as specified in the Hamburg data protection and privacy act (HmbDSG). The automatic forwarding of work emails, whose technical prevention is relatively straightforward, must therefore be considered a violation of Section 8 HmbDSG.

It must also be borne in mind that the data protection laws include a deletion obligation for personal data whose storage is inadmissible or that is no longer needed for the processor to perform its tasks. The University cannot effectively monitor compliance with this deletion obligation if emails containing relevant data are no longer stored within its sphere of influence, but rather on the servers of external email providers.

Protection of secrets pursuant to civil law

In a range of scenarios, the legal system recognizes that secrets are worthy of protection and, in some cases, provides for penalties against the perpetrator personally (fines or imprisonment) if this protection is violated.

With regard to the automatic forwarding of emails at universities, particularly violations of private secrets (Section 203 of the German Criminal Code, StGB) and breaches of official secrecy by public officials (Section 353b StGB) must be taken into account.

Labor law

From a labor law perspective, it should be noted that employees and civil servants are generally accountable to their employer in official or business matters and subject to the instructions given; however, exceptions are common in the field of research. Subject to these exceptions, they are obliged pursuant to the labor and civil service laws to present work emails to their employer upon request. As such, emails are generally compared to and equated with written documents and official mail.

Solution

Technically, the simplest solution would be to prohibit the automatic forwarding of work emails by staff and possibly also by students, whereby the aforementioned legal issues only arise in isolated instances for the latter. In particular, labor law aspects are irrelevant to students' email communication. Similarly, students belonging to one of the groups of persons listed in Sections 203 and 353b StGB (student employees or undergraduate research/teaching assistants) will probably be the exception, meaning that criminal law aspects can normally be disregarded.

We cannot uphold the current practice merely out of force of habit. Nor should the positive effects for the University's external image be underestimated if we can claim that sensitive data is in good hands with us and is not distributed around the world without reliable data usage control.

Recommendation

Prohibit the automatic forwarding of work emails for staff at Universität Hamburg and also prevent such services technically. Students should not be considered for the time being. A total of 1,764 automatic redirects are currently set up from staff accounts at Universität Hamburg to external email providers (above all Google), indicating an urgent need for action.

Sources and more information:

https://www.dfn.de/fileadmin/3Beratung/Recht/1infobriefearchiv/2015/Infobrief_Recht_06-2015.pdf

https://www.dfn.de/fileadmin/3Beratung/Recht/1infobriefearchiv/2015/Infobrief_Recht_07-2015.pdf