So you want to use Google Apps as a productivity suite for your business – seriously??

Lawyer Oliver Stutz proves that Google Apps for Work fulfils German data protection laws

This article originally appeared on the German blog datenschutz notizen (link to original). The author, Oliver Stutz, is an in-house lawyer at datenschutz nord, a German data protection and IT security company. Many thanks to Oliver Stutz for allowing us to publish this text on our blog in German and English!

In the words of Thomas Magnum, "I know what you're thinking, and you're right." – or, perhaps not. As consultants, we also found it difficult to approach this topic with open minds. Who – and this is a valid question in data protection terms – doesn't think of fire and water when they hear the terms "Google" and "data protection"? But does that still apply? This time, we aren't going to discuss the personal use of search engines, of Android and its many apps for personal use, or device-independent (universal) tracking, user profiling and other dubious technologies that impact data protection law. We will discuss the question of whether Google services (Google Apps for Work, Google Drive for Work, Google Apps Unlimited etc.) can really be used by businesses in a way that conforms to data protection laws.

Services in the cloud

The fact that these Google services are cloud-based in the purest sense needn't be discussed at length here. Likewise, the high demands of the *nschutzbeauftragte* (Federal Data Protection Ombudsman) outlined in *rungshilfe Cloud-Computing* (cloud computing first steps, e.g. here) will be familiar to our expert readership and are hence only briefly outlined below:

- the data processing service provider (outside the EU) must be SafeHarbor certified or enter into an agreement with the responsible authority according to the EU model contract clauses (notwithstanding that, substantively, the regulatory authorities – rightly (!) - consider SafeHarbor insufficient to guarantee a reasonable level of data protection in a third country)
- over and above the EU model contract clauses, the data processing service-provider has to provide details about any subprocessor, which includes
    - giving the names and locations of the sub-contractors, as well as

published at 2015-10-02

    - entering into an agreement with sub-contractors that binds them to the same data protection standards as the primary contractor
- further, the contractor must provide substantiated details of their technical and organisational security measures (which, in particular for cloud service providers, encompasses detailed information about the implementation of the data separation prerogative) and
- allow regular checks of their IT security
- finally, for the processing of sensitive data (HIPAA according to the US standard, or health - or other - data that are subject to doctor-patient confidentiality, are, for the sake of simplicity, assumed to be equivalent) there is an additional requirement that data be inaccessible even to system administrators.

And now I come to the central question: does Google fulfil all of that? Spoiler alert: it looks like it does!

Google's Whitepaper

Let's start with the document that directors and those with responsibility for IT in companies no doubt receive from Google as a "foundation" for all questions relating to data protection, IT security, and compliance: "Google for Work: Whitepaper zum Thema Sicherheit und Compliance". In this document, Google summarises all information on the aforementioned topics, namely:

- operational security
- IT security
- certification
- data use (access to data and restrictions)
- fulfilment of regulatory requirements, and
- pointers for users and system administrators for improving IT security.

Comparing the various contents against the aforementioned regulatory requirements, the first impression is positive (admittedly, scepticism cannot be entirely eliminated, more on that later). The fact that Google is SafeHarbor certified (also according to the bilateral agreement between Switzerland and the USA, by the way) is as well known as it is - from the authorities' standpoint, see above - meaningless. Despite the fact that one can thus assume that, on a bilateral level, **the company formally has a comparable standard of data protection to the EU**.

published at 2015-10-02

As an additional service for European customers, Google offers agreements incorporating the EU model contract clauses (Whitepaper, p. 15). So far, so good. But, bearing in mind the list of criteria above, so far we've only checked one item off our list. Let's turn our attention to the others ...

As far as the sub-contractors are concerned, Google readily discloses them here. And surprisingly, unlike e.g. Microsoft, the list is very short - so short that it is possible to name the companies here without imposing upon the reader too much: they are

- EPAM Systems Inc,
- Fujitsu Communications Services Limited,
- Sellbytel Group GmbH,
- Sutherland Global Services Inc.,
- Telus International (U.S.) Corp,
- Telus Communications Company und
- Voxpro Limited.

In order to examine the additional requirement that sub-contractors be bound to the same data protection standards as the principal contractor, we need to have a look at the document that Google calls the "Data Processing Amendment". **In the whitepaper, Google offers an opt-in to this amendment over and above the EU model contract clauses. I have to admit that I was surprised!** The amendment contains a (10-page, very detailed) contract on third-party data processing ("Data Processing Admendment to Google Apps Agreement"), also containing all the provisions that are not included in the EU model contract clauses but are necessary to make the legal permissibility "complete" - at least according to the regulatory authorities' undeniably relevant opinion. Section 11 of the document contains the following clause:

> 11.2. Processing Restrictions:
> Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that they are bound by written obligations (i) that require them to provide at least the level of data protection required by the Safe Harbor Privacy Principles; and (ii) if Customer (...) has entered into Model Contract Clauses with Google Inc. that impose the level of data protection required by the Model Contract Clauses.

As a supplement to that, section 5 of annex 2 on IT security (Subprocessor Security) states that all subprocessors must be subject to an audit to ensure that their IT

published at 2015-10-02

security measures are commensurate with the extent of their access rights and provided services.
Thus, where subprocessors are concerned, you couldn't really wish for anything more (legally).

IT Security

On the subject of IT security - where Google itself is concerned - the company is, within the limits of what is possible (detailed information on how access codes are generated or administered and how unique e.g. the authentication mechanisms are, is of course not made public) also surprisingly transparent. The second annex to the sub-processor contract contains exhaustive details about the infrastructure of the server farms, about the networks and secure means of data transfer, about access and physical access controls as well as about the (logical) separation of customer data and databases. Above and beyond this, **the Whitepaper gives customers exhaustive information about further measures for continually ensuring the highest possible IT security**, for example the fact that the security team alone consists of 500 people, and that there is a dedicated data protection team that audits products upon their launch and develops best practice solutions independently of the developer teams.

As a "hard fact", and bearing in mind the formal requirements for legally compliant subprocessing, the fact that the company is certified according to ISO 27001, SOC 2 and 3 as well as (in this context less relevant) FISMA (U.S. Federal Information Security Modernization Act) and FedRAMP (Federal Risk and Authorization Management Program, www.fedramp.gov) is of more significance.

Where monitoring of technical and organisational measures is concerned, section 6.4 of the amendment to data processing adds that the customer's right to perform their own security checks is satisfied by Google's proving that it has such certifications. Thus, the customer is not able to carry out their own audits. So if you're looking for the catch, this is where you'll find it - although comparisons with Microsoft (MS 365, Azure etc.) show that this approach to proving acceptable security is a standard amongst the large providers and in practice there is no real alternative.

Health data

Finally, the discussion wouldn't be complete without drawing attention the fact that **Google also offers its customers the ability to deal with Protected Health Information (PHI) separately.** To do so, it is necessary to opt in to a so-called

published at 2015-10-02

Business Associate Agreement (BAA, https://support.google.com/a/answer/3407054?hl=en). This ensures that PHI data (which, for the sake of simplicity, we shall deem to be the same as data that is subject to doctor-patient privilege) may only be stored in certain “core services”, to which Google administrators have no access. These core services include GMail, Google Drive (including Docs, Sheets etc.), Calendar and Google Apps Vault. Hangouts, Contacts and Groups are not core services. Detailed information on how to use these services for PHI is outlined in another exhaustive document, but should be viewed in a separate data protection context.

Conclusion

Perhaps I’m not the only one who is surprised at Google’s willingness to comply with German and European data protectors’ demands. As a consultant, in future **it will therefore be difficult to carry on advising businesses against using Google for Work so long as they enter into all of the aforementioned bilateral agreements with Google**. It may be the case that Microsoft has a head start on Google with regard to trust amongst businesses that want to move into the cloud come hell or high water (even if this cannot be justified by regulations) - but this head start is likely to shrink even more.

---

plus3trainings GmbH from Hamburg, Germany delivers professional services in projects with trainings and webinars + change management + project support + consulting + coaching
We do trainings + local client communication + prepare and translate training material + documentation and change management for international partners in Germany.
Contact +49 40 22869842 + https://www.plus3trainings.eu + info@plus3trainings.eu

published at 2015-10-02