ERNW

Newsletter 52 / February 2016

Fried wart Kuhn

Digital unterschrieben von Friedwart Kuhn
Datum: 2016.02.17 17:11:07 +01'00'

Some Recommendations Regarding Windows 10 Privacy Settings

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4

69115 Heidelberg

Tel. +49 6221 480390
Fax +49 6221 419008
www.ernw.de

Version: 1.0

Date: 2/17/2016

Author(s): Friedwart Kuhn, Florian Gattermeier, Nina Matysiak, Heinrich Wiederkehr

ERNW
providing security.

TABLE OF CONTENT

1 INTRODUCTION

Privacy in the context of information technology usually refers to the protection and control over the access to one's own personal data. This is also what is covered by data protection laws. The European Data Protection Directive, which has to be implemented by national law within the European Union, defines personal data the following way: "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;".[1]

So, in the legal sense, personal data does not include all data worth of protecting, as for example business plans. The collection, storage and analysis of personal data is going to be problematic, if the data subject does not give his or her voluntary and informed consent to it. Especially the "informed" part is what data privacy experts criticize about the general Microsoft privacy statement[2], which also describes Microsoft's approach in Windows 10, by claiming that it is not transparent enough regarding what data is collected, for which goal and how to object to it.[3]

While criticism of Microsoft's privacy policy was already widespread with the release of Windows 8.1 and the introduction of Smart Search, the public discussion reached a peak with the release of Windows 10 default integration of features such as OneDrive[4]. Although the user can customize the privacy settings to minimize the amount of data shared with Microsoft and installed apps (Windows apps as well as third-party apps), it was criticized that Microsoft did not decide to follow a privacy by design approach. Instead, Microsoft opted to go for loose privacy settings by default, combined with an opt-out policy, which does not even give the opportunity to entirely prevent the flow of privacy-related data to Microsoft.

The discussion gained further momentum with the release of the optional patches KB3068708, KB3022345, KB3075249 and KB3080149 for Windows 7 and Windows 8/8.1. These "patches" have been suspected to backport data collection and telemetry services functionality implemented in Windows 10 to Windows 7/8/8.1. A closer look showed that these patches related mainly to the diagnostics services for customers that participate in the Customer Experience Improvement Program (CEIP) - which is for most applications an opt-in process and can be switched off entirely via the control panel. But patch KB3075249 added telemetry points to the User Account Control (UAC) feature to collect information on elevations that come from low integrity levels.

Privacy settings can be set via the GUI and Group Policies (or directly in the Windows registry). In enterprise environments, the distribution of settings via Active Directory-defined Group Policies is the standard deployment process of settings that have to be applied enterprise-wide. Thus, administrators are able to enforce configurational settings, and users without administrative permissions on their systems are not able to change these settings.

Some of our customers turn off everything, but this is not necessarily needed for a good level of security *and* privacy. If you don´t turn off all the privacy-related stuff completely, you should know the potential privacy impact. In case of doubt, the data security officer of your organization should be consulted. To make the decision easier for you, we have created an extensive sheet that covers each possible privacy setting together with a recommendation. It can be found in our official ERNW development channel at GitHub.[5]

[1] *See* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
[2] *See https://privacy.microsoft.com/en-us/privacystatement/.*
[3] *The Federal Data Protection Law (BDSG) is even stricter than the EU directive and it is likely that the chosen opt-out policy might pose a violation of the BDSG. But whether the collection of data by Microsoft falls into the jurisdiction of the BDSG depends on where the settlement of the responsible body for the data collection is placed. If it is placed in another state that is a member of the EU or EAA, the data protection laws of this state will apply.*
[4] *OneDrive is installed by default, but only usable in combination with a Microsoft account. Officially, Microsoft strongly recommends the usage of such an account, so in many cases an active OneDrive will be the default state.*
[5] *See https://github.com/ernw/insinuator-snippets/tree/master/Win10-privacy.*

2 PRIVACY SETTINGS

Let's move on to the technical perspective and have a short overview about the privacy settings and their categories.

2.1 Microsoft Account & OneDrive

Azure Active Directory (for enterprises) and Microsoft account (for consumers) are Microsoft's cloud-based directory and identity management services, which give organizations and consumers single sign-on experience. To use these services, a Microsoft account is mandatory. The risk potential of a logged-in Microsoft account goes along with several synchronization features, which may possibly share sensitive account information with all your devices – and Microsoft. For example, credentials can be synchronized to the cloud and to other systems that are using the specific Microsoft account.

Microsoft OneDrive is another synchronization service that comes built-in with Windows 10 and provides a similar experience to cloud storage services like Dropbox or Google Drive. By default, OneDrive is active and can be used for several purposes, such as saving documents and pictures or backing up the BitLocker recovery key. Here it should be kept in mind that this might violate the requirements resulting from your organizational data classification.

If you do not need to use any of these services, we recommend to turn them off and prohibit users (via GPO setting) to log in with a Microsoft account. Remember that the Windows App Store also requires a Microsoft account and therefore it is not possible to load or update apps from it. In order to get more granular control over the Windows store and all apps, you will need to use the Windows Store for Business[6] (e.g. app and license management).

2.2 WiFi-Sense & Hotspot-Authentication

WiFi-Sense enables automatic login to known Wi-Fi networks and sharing of Wi-Fi credentials to Facebook, Outlook and Skype contacts. The criticality of this feature is out of doubt and the default configuration of WiFi-Sense is a highly problematic one. Imagine an employee of your organization, using his or her corporate notebook (with the credentials for the corporate WiFi) for personal activities (if this is allowed), like communicating via Skype or Facebook: WiFi-Sense will share the corporate's WiFi credentials to all contacts of the employee in Facebook, Skype or Outlook!

[6] *See https://www.microsoft.com/en-us/business-store/.*

The following screenshots show an exemplary WiFi-Sense configuration:

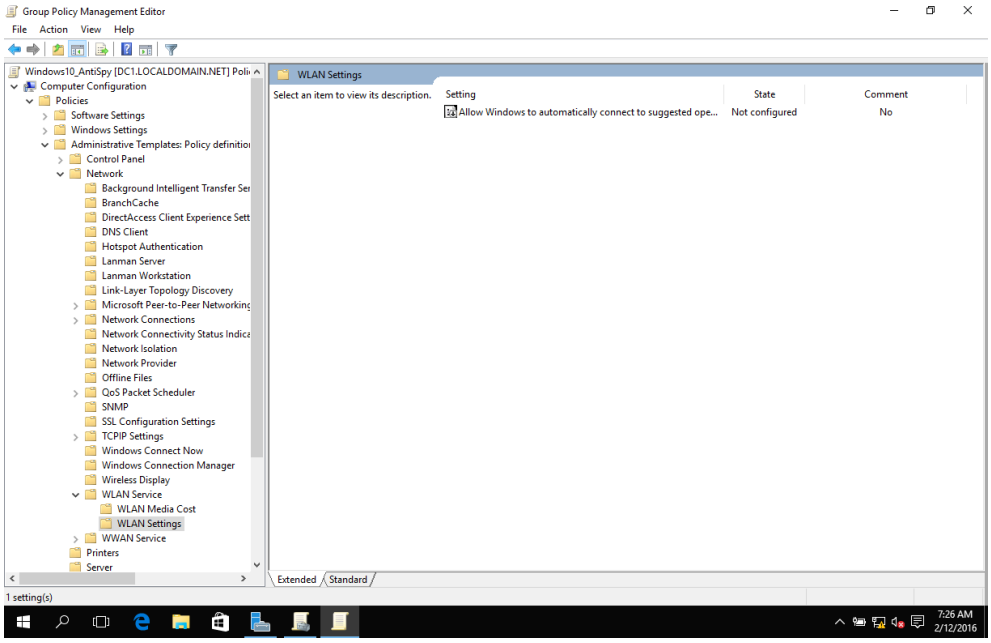

Figure 1 Default configuration of WiFi-Sense

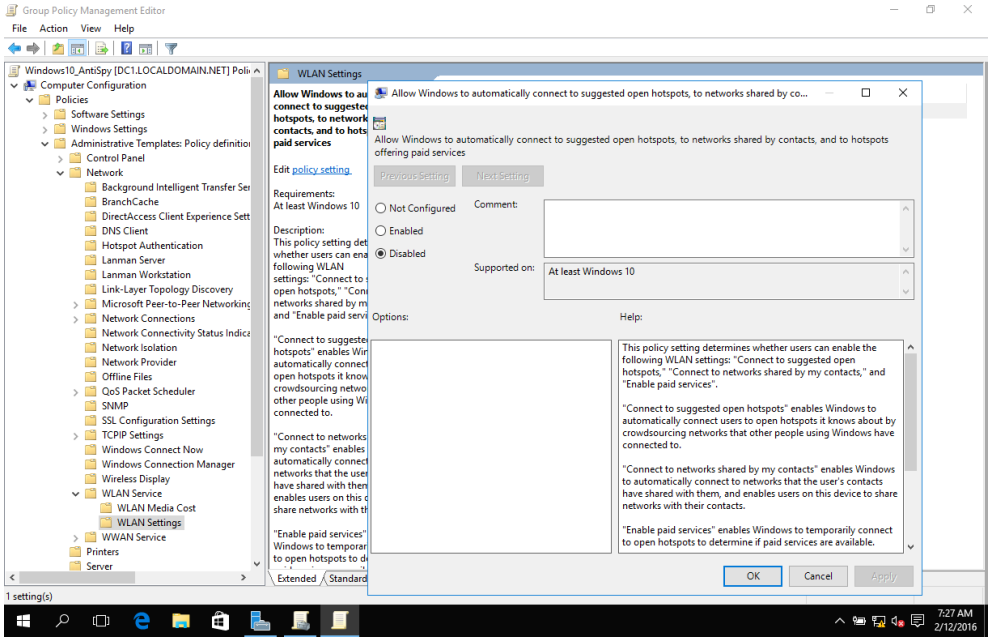

Figure 2 Recommended configuration of WiFi-Sense

2.3 Telemetry, Feedback & Diagnostics, CEIP, Error Reporting

Regarding Error Reporting you might completely disable any data traffic to Microsoft, but even if the default configuration is kept, Windows asks the user before sending data. For most applications the Consumer Experience Improvement Program (CEIP) is opt-in but regarding Windows itself it is opt-out. You can opt-out during the installation process or afterwards. If you take part in CEIP, Microsoft collects information about your device, as well as connected devices, how you use the program for which you participate and how it is set-up and performing during runtime. To perform a proper analysis of the collected reports over time, CEIP creates a globally unique identifier (GUID), which is stored on your system and is sent with every report. The GUID is randomly generated and does not include any information about your device. However, the collected data might contain identifying information (such as a serial number of a connected device), which could make it possible to establish a link between your device and your GUID. Telemetry, as well as Feedback and Diagnostic, cannot be turned off completely. It is not possible to opt-out entirely of sending any data to Microsoft. For Windows 10 Enterprise, Windows 10 Education, Windows 10 Mobile Enterprise and IoT Core the lowest level available is the "security level", which still includes information about the OS version used, the device ID, the device class and, if it is used, the Malicious Software Removal Tool (MSRT) (including device info and the IP address) and the Windows Defender (including: anti-malware signatures, diagnostic information, User Account Control settings, Unified Extensible Firmware Interface (UEFI) settings, and IP address). For other editions the lowest selectable level is the "basic level", which includes additional information[7] about the device on which Windows is running.

The following screenshots show an exemplary telemetry configuration:

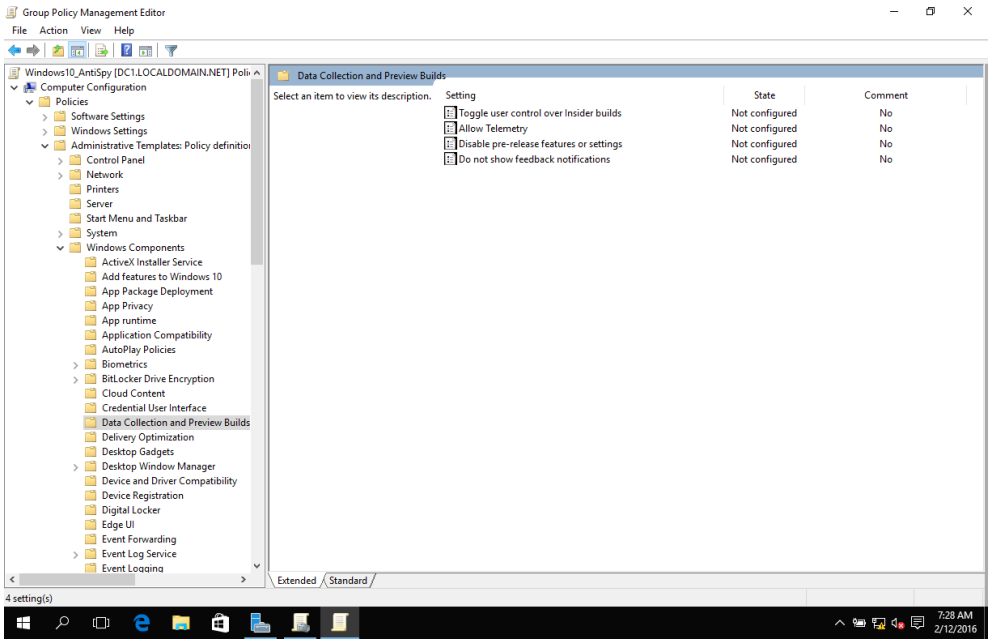

Figure 3 Default telemetry configuration

[7] *See* https://technet.microsoft.com/en-us/library/mt577208(v=vs.85).aspx#BKMK_UTC_Basic.

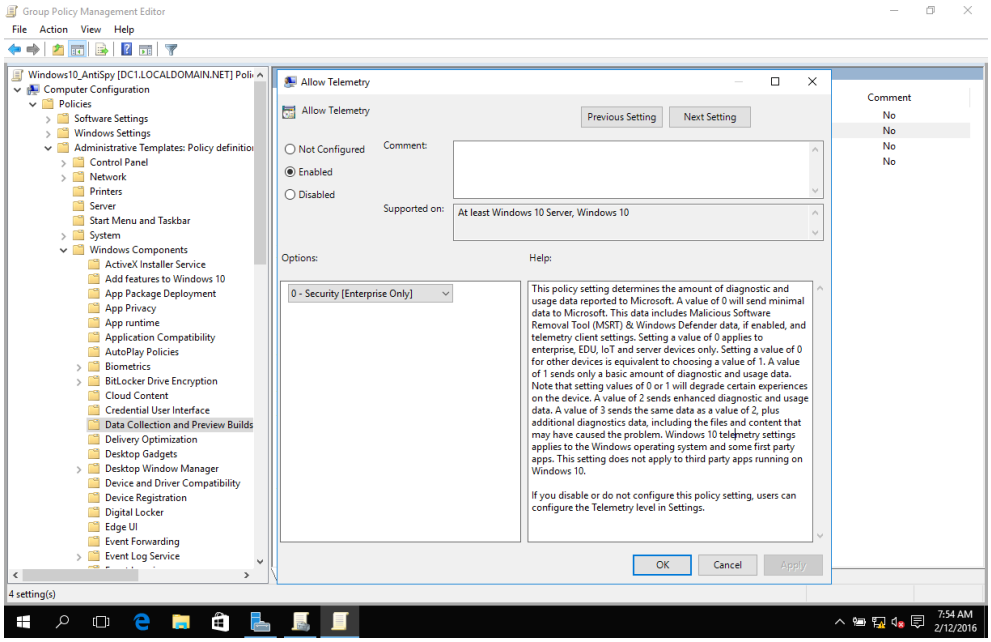

Figure 4 Recommended telemetry configuration

2.4 Personalization features

Depending on the device type, in particular tablet devices with touch input and voice recognition, handwriting personalization and other adapting techniques like speech pattern recognition could lead to serious business risks (e.g. when corporate business data from a meeting is analysed in the Microsoft cloud for handwriting personalization). Microsoft is planning to use German datacentres in cooperation with the Deutsche Telekom, but currently all traffic related to personalization features (including what you speak and what you write) ends on servers outside of Germany.[8] Hence, if you do not want to share your data with Microsoft, turn off such features.

2.5 Targeted Ads

Having "Personalized ads wherever I use my Microsoft account" active is the "simple" description of a wide-spanning setting. Having personalized ads turned on means that Windows 10 itself becomes a hub for targeted ads. To set a cookie for your browser, which deactivates this feature, go to https://choice.microsoft.com/en-gb/opt-out and set both options to "off". You should keep in mind, that this deactivates personalized ads only in the browser! For a complete deactivation of this feature set, the "advertising ID" should be turned off via Group Policy.[9]

2.6 Location

Location-aware applications can track movement by monitoring the built-in location sensor (GPS sensor). With that information, the application can create a detailed motion profile. So it is a good idea to turn location access completely off, if you do not need to use it. Otherwise, only apps that really depend on location-based functionalities (like maps or navigation) should have access to the location sensors. This can be granularly adjusted with the settings in the following section.

---

[8] *See* http://news.microsoft.com/europe/2015/11/11/45283/ *and* https://azure.microsoft.com/de-de/regions/.

[9] *In November '15, an upgrade to the latest build of Windows 10 (TH2, build 1511) reverted the user's advertising, SmartScreen and synchronization settings, which were set via GUI on personal builds (Home, Pro) of Windows 10. Corporate environments were not affected because of the management of these settings via Group Policy. Nevertheless, this was not the intent of Microsoft and a statement from Microsoft was released (see* https://support.microsoft.com/en-us/kb/3121244*).*

2.7 Cortana, Windows Apps, App Privacy

Cortana is a personal assistant, which Microsoft included with Windows 10, and for full functionality it needs plenty of information about you. You still can deactivate different options of information gathering, but without voice recognition, location determination, contact information etc. Cortana might not be very useful. The information Cortana gathers to "get to know you better" is stored in "Cortana's notebook" on your system and in the cloud. You can delete the "notebook" manually, but voice data without personal references is nevertheless stored for 30 days to improve services that use voice recognition. If you use Cortana, Microsoft apps and services have access to the collected data, third-party apps and services as well if the user permits it. Microsoft states that none of the collected data is passed on to advertisers.[10] If you choose to use Cortana, be aware that you might disclose not just your own personal data to Microsoft but also data of your contacts.

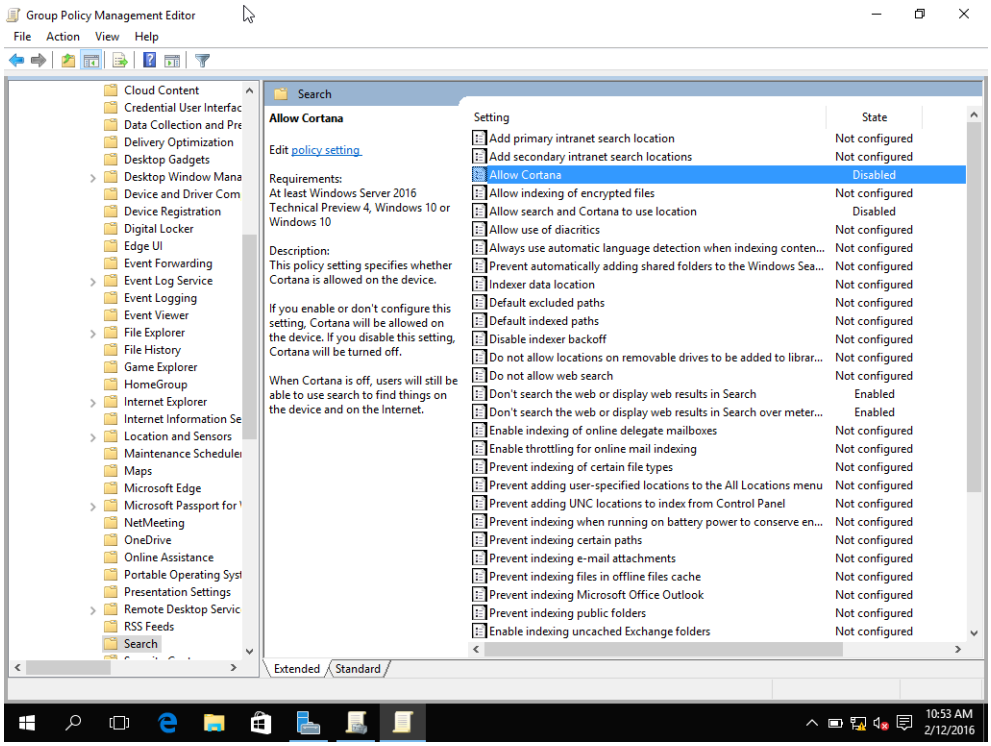

Figure 5 Recommended Cortana and search configuration

[10] *See http://windows.microsoft.com/en-us/windows-10/cortana-privacy-faq.*

If it is intended to use Windows apps in your organization, you should configure the GPOs regarding App Privacy to customize the access of apps to resources and data on your device like it is shown in the screenshot below. Keep in mind that some apps may rely on access to ensure their functionality. Then again, if you don't plan to use Windows apps, we recommend to remove the Windows Store. But access to the Windows Store is required to install updates for apps, so just deny access or remove the Windows Store if you no longer have any apps installed.

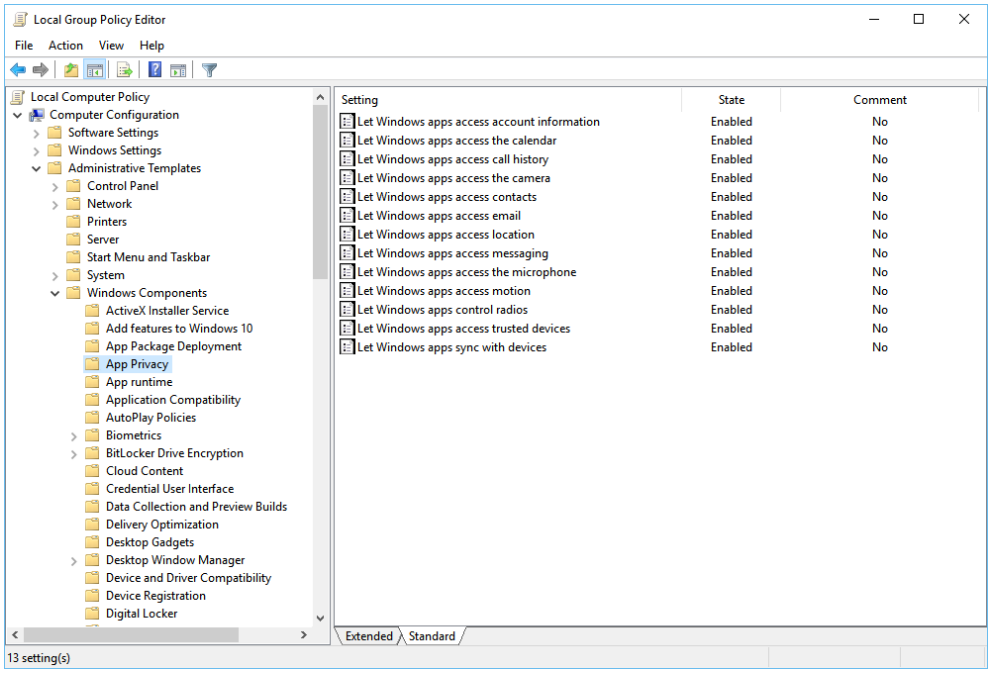

Figure 6 Recommended app privacy settings (Enabled allows for a granular configuration of the settings)

3 OPERATIONAL IMPACT

Good news: As for the operational impact of the recommended settings it might be stated that the impact is generally low to negligible. There are only few exceptions of this statement:

- Deactivation of Windows Store prohibits app updates.
- Some organizations might allow usage of OneDrive, thus the recommended deactivation will contradict this, but as for many other recommended settings, enterprises will mostly not allow this.
- Same for Cortana: Some apps might use Cortana (e. g. dictate e-mails), but we recommend to not store speech data in the Microsoft cloud.

If you have further questions or you if want to comment on this topic, feel free to contact us.

As it is already late February, TROOPERS16 is just around the corner! The conference itself is unfortunately already sold-out, but you still have the chance to sign-up for one of the many great workshops. If you are interested in knowing more about how to secure your Microsoft environment, join us at our "Hardening Microsoft Environments" workshop on 14th and 15th of March, some seats are still available (*https://www.troopers.de/events/troopers16/570_hardening_microsoft_environments/*). We are looking forward to seeing you (again) at TROOPERS16!

All the best from the ERNW Microsoft security team,

Friedwart, Florian, Nina, Heinrich, Dominik.

4 APPENDIX

4.1 Disclaimer

All products, company names, brand names, trademarks and logos are the property of their respective owners.