JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Syynimaa, Nestori; Viitanen, Tessa

Title: Is My Office 365 GDPR Compliant? : Security Issues in Authentication and Administration

Year: 2018

Version: Accepted version (Final draft)

Copyright: © Syynimaa & Viitanen & SCITEPRESS, 2018.

Rights: In Copyright

Rights url: http://rightsstatements.org/page/InC/1.0/?language=en

Please cite the original version:

Syynimaa, N., & Viitanen, T. (2018). Is My Office 365 GDPR Compliant? : Security Issues in Authentication and Administration. In S. Hammoudi, M. Smialek, O. Camp, & J. Filipe (Eds.), ICEIS 2018 : Proceedings of the 20th International Conference on Enterprise Information Systems. Volume 2 (pp. 299-305). SCITEPRESS Science And Technology Publications. https://doi.org/10.5220/0006770602990305

Is My Office 365 GDPR Compliant?
Security Issues in Authentication and Administration

Nestori Syynimaa[1,2,3] and Tessa Viitanen[4]
[1]*Faculty of Information Technology, University of Jyväskylä, Jyväskylä, Finland*
[2]*Gerenios Ltd, Tampere, Finland*
[3]*Sovelto Plc, Helsinki, Finland*
[4]*Unified Chargers Ltd, Espoo, Finland*

Keywords: Office 365, Azure, Information Security, GDPR.

Abstract: The General Data Protection Regulation, commonly referred as GDPR, will be enforced in all European Union countries in May 2018. GDPR sets requirements for processing EU citizens' personal data regardless of the physical location of the organisation processing the data. Over 40 percent of European organisations are using Office 365. Microsoft claims that Office 365 service is GDPR compliant, and has provided tools to help Office 365 customers to ensure their GDPR compliancy. In this paper, we present some security issues related to the very foundation of Office 365 service, namely Azure Active Directory and administrative tools, and assess their GDPR compliancy. Our findings reveal that personal data stored in Office 365 is subject to undetectable security breaches, preventing organisations to be GDPR compliant. We also propose actions to take to minimise the impact of the security issues.

1 INTRODUCTION

The General Data Protection Regulation, or GDPR, will be enforced in all European Union (EU) countries on May 25th, 2018. The purpose of GDPR is to allow EU citizens to control their personal data better. It sets certain requirements for all organisations handling personal data of EU citizens regardless of the location of the organisation. If organisations fail to comply with GDPR, they may be subject to a fine of 20 million euros and up to 4% of the total annual turnover, or even impose a temporary or definitive limitation including a ban on processing the personal data.

Office 365 is Microsoft's cloud service used by many organisations worldwide. In 2016, over 22% of enterprise users were actively using Office 365 worldwide (Skyhigh, 2016). In Europe, the adoption rate was 43% (Bitglass, 2016), so its data protection capabilities affect many organisations' GDPR compliancy.

According to Microsoft (2017d), the Office 365 service is GDPR compliant, and they provide tools for their customers to be GDPR compliant. The tools help organisations to find personal data from the Office 365 services, such as Exchange Online and SharePoint Online, and to assess and build relevant controls. However, little is known about the compliance of the very foundation of Office 365 service, such as Azure Active Directory and management tools. In this study, we assess GDPR compliancy of the foundations of Office 365 from the customer point-of-view. This is crucial because organisations are responsible for their GDPR compliancy, not their service providers, such as Microsoft. Moreover, the Microsoft Online Services Agreement limits Microsoft's liability (Tomisek, 2015).

The rest of the paper is structured as follows. In the second section, we will introduce GDPR and how it affects organisations. In the third section, details of Office 365 relevant to GDPR are described in detail. In the fourth section, we will present the GDPR compliancy assessment of Office 365. Finally, in the fifth section, we will discuss our findings and propose some recommended actions for Office 365 organisations to take.

2 GENERAL DATA PROTECTION REGULATION (GDPR)

General Data Protection Regulation (GDPR) is a regulation for the EU citizens to better control their personal data (European Union, 2016. hereinafter GDPR). In this section, we will introduce GDPR aspects relevant to this study.

2.1 Key Points and Terminology

For EU citizens, GDPR means that they will have *easier access to their data*, including more information on how their data is processed. They will have a *right to move data* (GDPR Article 20) between service providers, and a *right to be forgotten* (GDPR Article 17). Most importantly, they will have a *right to know when their personal data has been breached* (GDPR Article 33). However, the notification is mandatory only in a case when it is likely to result in a high risk to the rights and freedoms of natural persons.

Table 1: GDPR terminology (GDPR Article 4).

Term	Definition
Personal data	Information related to a natural person (data subject)
Processing	Any operation performed on personal data
Controller	The body which determines purposes and means for processing the data.
Processor	The body which processes data on behalf of the controller.
Recipient	The body to which the personal data is disclosed
Consent	Freely given indication of the data subject's wish to signify agreement to processing of personal data
Personal data breach	Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
Representative	Person representing controller or processor
Enterprise	Natural or legal person engaged in an economic activity
Supervisory authority	Independent public authority

For organisations, this means a couple of requirements. For instance, they must *perform impact assessments* (GDPR Article 35) in a case of the high risk involved, and *keep records of data processing activities*.

The GDPR terminology used in this study is presented in Table 1.

2.2 Requirements for Organisations

The data subject, i.e., a natural person, has a right to know the recipients to whom the personal data is disclosed (GDPR Article 15(1)). This means that organisations must know who is processing the data. More specifically, organisations are responsible for implementing appropriate measures to ensure and to be able to demonstrate how the processing is performed (GDPR Article 24). Organisations must also record the processing activities (GDPR Article 30 (1-4)).

All personal data must be protected by design and by default. This means that organisations are responsible for ensuring that by default, the data is not made accessible to an indefinite number of people without individual's intervention (GDPR Article 25).

Organisations must use processors in such manner that processing will meet the requirements of GDPR (GDPR Article 28 (1)). Moreover, all processors must be governed by a binding contract (GDPR Article 28 (3)).

Before starting processing the data, for instance when new software is used, the organisation is responsible for performing a data protection assessment (GDPR Article 35). In case of uncertainty, prior consultation is needed (GDPR Article 36).

Organisations are responsible for reporting a personal data breach to supervisory authority without

Table 2: Summary of GDPR requirements for organisations.

Requirement
Awareness of who is processing the personal data
Keep record of processing activities
Personal data not accessible to an infinite number of people
Use only processors in a manner that processing will meet the requirements of GDPR
Processors must be governed by a binding contract
Perform a data protection assessment
Ability to detect personal data breach
Report personal data breach without a delay

delay in 72 hours (GDPR Article 33 (1)) and to the data subject without delay (GDPR Article 34). This means that organisations need to be able to detect such a breach.

The summary of GDPR requirements for organisations is presented in Table 2.

3 OFFICE 365

Office 365 is a cloud-based subscription service consisting of Office suite applications, such as Excel and Word, and server products as a service, such as Exchange and SharePoint (Microsoft, 2017g). There are many different combinations of the services, packaged and sold as *subscriptions*. For instance, *Office 365 Business* subscription contains only Office suite and OneDrive service, whereas *Office 365 Enterprise E3* subscription contains Office suite and the full set of server software, including Exchange and SharePoint. There are also subscriptions for government and education sectors.

3.1 Domains

When an organisation acquires a subscription for the first time, an Office 365 *tenant* is created. The tenant can have multiple subscriptions, so it is possible to have E3 above for office workers and web-based email for others. When creating a tenant, a unique name needs to be chosen, such as MyCompany, which creates a tenant named mycompany.onmicrosoft.com. This tenant name cannot be changed afterwards, and it is also the initial domain of the tenant. This means when creating a user, such as John Doe, his login name could be john.doe@mycompany.onmicrosoft.com. This login name is also called a User Principal Name (UPN), which is a unique name of the user across the whole Office 365 service.

Organisations can also add their domains to Office 365 tenant, such as mycompany.com. There is a verification process to be completed before the domain can be used. The verification requires access to domain's Domain Name Services (DNS) to create required DNS records. After the domain is verified, users can configure to use that domain. For instance, John Doe could now have a UPN john.doe@mycompany.com.

Domains in Office 365 can be used for authentication and email addresses. Users have only one login name but may have multiple email addresses or aliases.

3.2 Azure Active Directory

Every Office 365 tenant has an associated Azure Active Directory (AAD). Every user added to Office 365 will have a user object in AAD. Moreover, each user objects have a set of attributes, containing information related to the user. Attributes containing personal data are listed in Table 3.

Table 3: Azure Active Directory user object attributes.

Attributes	
AlternateEmailAddresses	AlternateMobilePhones
AlternativeSecurityIds	City
Country	Department
DisplayName	Fax
FirstName	ImmutableId
LastName	Licenses
LiveId	MobilePhone
ObjectId	Office
PhoneNumber	PostalCode
PreferredLanguage	ProxyAddresses
SignInName	State
StreetAddress	Title
UsageLocation	UserPrincipalName

3.3 Administration Roles

Each user object in AAD has an associated administrative role. The default administrative role is *user*, which have no administrative rights at all. They can log in to Office 365 and use the services they are licensed to use. Other basic administrative roles are listed in Table 4. There are also other administrative

Table 4: Azure Active Directory Administration Roles (Microsoft, 2017a).

Role	Description
Global administrator	Access to all administrative features. The only role that can assign administrative roles to others.
Billing administrator	Can purchase subscriptions and licenses, and see billing information.
User management administrator	Can create and delete users, change passwords, and assign licenses, except for roles above. Can create, manage, and delete groups.
Password administrator	Can reset passwords for non-administrator users.
Service administrator	Can open support tickets and have read-only permission to administrative features

roles, such as Exchange administrator, but these roles are not relevant to this study.

There are two types of administrative interfaces: web-based admin centres and PowerShell. The former can be accessed by any supported web browser, such as Edge, Firefox, and Chrome. Admin centres are suitable for the most of the administrative tasks but do not support any automated or bulk actions. For automation and command line administration, there is a PowerShell module for AAD, Exchange, SharePoint, and Skype for Business. PowerShell allows administrators to perform all administrative tasks, including bulk editing of users.

3.4 Delegated Administration

Delegated Administration is an arrangement where Office 365 customer has delegated administrative rights to some Microsoft partner organisation. This requires a contract between the partner and customer organisations. Technically the partner organisation sends a delegated administration offer to customer's administrator, who accepts the offer. After that, the partner organisation can perform administrative tasks on behalf of the customer.

Microsoft partner organisations have two extra administrative roles they can assign to their users. These are *Full administration*, having *global administrator* rights to customers' tenants, and *limited administration*, having *password administrator* rights to customers' tenants.

3.5 Identity Models

Office 365 uses the associated AAD for two purposes: to manage and authenticate users. Currently, there are three identity options to choose from: Cloud identity, Synchronized identity, and Federated identity (Microsoft, 2017f).

In cloud identity, the user accounts are managed in Office 365 only. When users are logging in, their credentials, i.e. username and password, are checked against the AAD.

In synchronised identity, the user credentials are checked against the AAD. However, some or all users are managed in an on-premises Active Directory (AD) and synced to AAD. The synced users will have the same username than in on-premises AD. Also, the passwords can be synced so that users can have identical credentials than in on-premises AD. This is sometimes referred as same-sign-on.

In federated identity, the user objects are synchronised to AAD, but the authentication takes place in an on-premises server. Usually, this is implemented using Active Directory Federation Services (AD FS). Federated identity is often referred as the most secure identity model because no passwords are sent to Microsoft, and the authentication method can be freely chosen. If configured properly, federated identity provides a true single-sign-on experience.

The federated identity is domain specific, i.e., all users having the specific domain are federated. However, the tenant may have multiple domains each using its own identity model. So, they may be a mixture of cloud identities, synced identities, and federated identities. The initial domain of the tenant, such as mycompany.onmicrosoft.com, cannot be federated.

There is also a recently announced fourth identity model called pass-through identity. This is similar to the federated identity as the authentication takes place in an on-premises server. In this model, the authentication is performed by an agent installed on the on-premises server. The agent opens a connection to AAD and credentials are checked using the connection. However, due to current limitations (Microsoft, 2017b), this model requires synchronised identity with password synchronisation for all services to work.

4 OFFICE 365 AND GDPR COMPLIANCY

Organisation requirements set by the GDPR can be summarised into three categories. First, organisations must know and keep a record of who is processing the data. Second, organisations must use only processors that have the knowledge of the GDPR and are governed by a legally binding contract. Third, organisations must be able to detect personal data breaches.

For regular customer controls, Microsoft provides Compliance Manager to help their customers to be GDPR compliant (Microsoft, 2017c). This covers services such as Exchange and SharePoint., but not the foundation of Office 365, such as AAD and administrative tools. We will next assess these areas.

4.1 PowerShell Administration

As mentioned earlier, there are several PowerShell modules to administer different Office 365 services. For instance, to manage users and their licenses in Office 365, one uses *MSOnline PowerShell module*

for Azure Active Directory. With the module, administrators can, for instance, perform following administrative tasks:

- Manage users and groups
- Manage domains
- Manage administrative roles
- See available subscriptions and licenses

According to documentation, the module requires a user having an administrator role (Microsoft, 2017e). In reality, this is not the case. Any user in the AAD can connect to Office 365 using the MSOnline PowerShell module. However, users have read-only access to all information, but they are not able to manage anything.

The read-only access gives users the ability to read and export all data the MSOnline PowerShell has access to. This includes user objects and the personal data listed in Table 3. To access the data, the user needs to install the PowerShell module following instructions at http://aka.ms/aadposh. After installation, users can run the following two-line script to export all user data from the AAD to their local computers.

```
1: Connect-MsolService
2: Get-MsolUser | Export-Clixml
   -Path users.xml
```

Besides reading all the user data, users can also list administrators having a specific role. For instance, the following two-line script lists all administrators having a Global Administrator rule.

```
1: $roleid=Get-MsolRole -RoleName
   "Company Administrator"
2: Get-MsolRoleMember
   -RoleObjectId $roleid.ObjectId
```

The PowerShell access cannot be currently prevented. Moreover, access is not logged anywhere, and therefore it cannot be detected. As a result, if the user object contains any personal data, the organisation does not comply with GDPR, as the data can be accessed by anyone in the organisation without detection. Also, organisations cannot be sure that the personal data is processed accordingly. If an organisation has created accounts for external users in their Office 365 tenant, some users might not be even governed by a binding contract.

4.2 Delegated Administration

As mentioned earlier, Office 365 customers can delegate their administrative tasks to one or more Microsoft partner. The delegated administration requires a contract, which can be terminated by the customer at any time. The customer can see all delegated administration contracts, i.e., the names of the partners, as illustrated in Figure 1. However, customers cannot see which administrative rights the partner has assigned to partner's own users. This means that the organisation does not know who has administrative rights to their organisation or who have assigned those permissions. Thus, it is likely that there are administrators who are not governed by a binding contract. Moreover, partners can access organisation's Office 365 tenant using PowerShell, so all issues introduced in the previous sub-section are also applied. As a result, organisations having delegated administration contracts does not comply with GDPR.

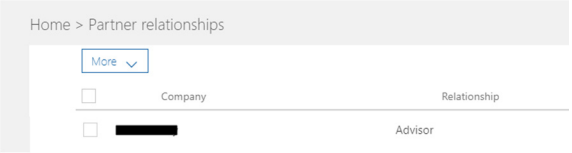

Figure 1: Customer's view of partner relationships.

4.3 Federated Identity

Recently a security vulnerability related to federated identity was discovered and revealed by the lead author of this paper (Syynimaa, 2017). The vulnerability is related to how Office 365 handles the federation trusts.

As mentioned earlier, the federation is domain based. For instance, there might be two domains, such as mycompany.com and mycompany.net. We can choose the identity model for domains separately. For instance, we can use synced identity for mycompany.com and federated identity for mycompany.net. When a domain is configured as federated, a trust is formed between Office 365 and on-premises federation server. This trust includes information on the location of the federation server and a digital signature. The location is typically in the form of https://sts.mycompany.net. When a user is logging in to Office 365 using for instance name john.doe@mycompany.net, Office 365 redirects the user to the federation server. When the user is authenticated, the federation server creates a security token for the user. The security token contains claims about the user, i.e., user's UPN and ImmutableId. The latter one is user's on-premises AD objectId in Base64 encoded format. When the user is returned to Office 365, the security token and its signature are checked against the trust information. If everything matches, the user is allowed to access Office 365.

The security vulnerability mentioned earlier

revealed that the federation trust is tenant wide. This means that any federation server can authenticate users on any domain of the tenant. This also covers the users having the initial mycompany.onmicrosoft.com domain and external users. External users are users to whom organisation users have shared for instance documents in SharePoint.

This means that any administrator having a Global Admin role can access, modify, and create any data using the identity of any user, provided that the user has rights to do so. To do this, the administrator can use an existing domain of the tenant, or add and verify a new one, such as mydomain.net. The first step is to install and configure a Windows server, for instance to a Windows 10 computer having Hyper-V enabled. The server needs to be promoted to a domain controller, and the AD FS role needs to be added and configured. When the server is properly configured, the administrator can install the MSOnline PowerShell module to be able to connect to Office 365 from the server. When completed, the administrator can run the following two-line script to convert a domain to federated:

```
1: Connect-MsolService
2: Convert-MsolDomainToFederated
    -DomainName mydomain.com
```

Now the domain is converted to federated, and the trust is formed between Office 365 and the federation server. Next step is to forge AD FS server's claim issuance rules to provide UPN and ImmutableId of the user the administrator wants to log in as (for details, see Syynimaa, 2017). When the administrator browses to Office 365 and gives username such as someone@mydomain.net (the user does not need to exists) the browser is redirected to administrator's AD FS server. After logging in as any local user on AD FS server, the administrator is given access to Office 365 as the user defined in the claim issuance rules.

Because everything above is performed on administrator's own computer, it cannot be prevented nor detected in any way. To increase security in Office 365 and Azure AD, it is possible to configure a multi-factor-authentication (MFA). If configured, after the user has logged in using username and password, MFA prompts for a one-time access code or makes a phone call to the user. However, the security vulnerability allows the administrator to bypass MFA. As a result, if the organisation has any Global Administrators (all organisations has at least one), they are not GDPR compliant.

5 DISCUSSION

5.1 Conclusions

GDPR sets many requirements for processing the personal data. It covers all processing, including the data in Office 365. The issues presented in this paper; the PowerShell administration, delegated administration, and federated identity vulnerability, prevents organisations being GDPR compliant.

Microsoft has put a lot of effort on tools, such as Compliance Manager (Microsoft, 2017c), to help their Office 365 customers to be GDPR compliant. However, those tools do not pay any attention to the very foundations of the service, as demonstrated in this paper.

5.2 Implications

In this paper, we have presented information security issues of Office 365 and Azure AD. As such, our findings help organisations to assess their high-risk data processing compliance, as required by GDPR Article 25. As we have demonstrated, the personal data is subject to security breaches. Therefore, organisations should not process any high-risk personal data in Office 365, until the security issues are fixed.

5.3 Limitations

The study covers only the very foundations of Office 365 service, namely Azure Active Directory and administrative tools. The general customer controls were out-of-scope of this study. For instance, by default, users can synchronise the content of their OneDrive, and any SharePoint site they have access to, to their personal computer. As a result, organisation's data is made accessible to anyone using that computer. This can be prevented by limiting synchronisation only to domain-joined computers.

5.4 Recommended Actions

Organisations synchronising their users from on-premises Active Directory to Azure AD should stop syncing attributes having personal data until the PowerShell access is limited to administrators only. This might have some negative usability effects for instance in SharePoint online as all attributes are not available.

Organisations having delegated administration contracts should revoke those contracts immediately.

Organisations can create administrator accounts to their Office 365 tenant for partner organisation's users as needed. This way organisation has full control of the administrator accounts.

All organisations should remove all unnecessary Global Administrator rights immediately to minimise the risk of exploitation of the identity federation security vulnerability.

REFERENCES

Bitglass. (2016). *Cloud Adoption EMEA* (pp. 10). Retrieved from https://pages.bitglass.com/rs/418-ZAL-815/images/BG%20Report%20-%20EMEA%20Cloud%20Adoption%202016.pdf

European Union. (2016). L119, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union, 59*(4 May 2016), 1-88.

Microsoft. (2017a). About Office 365 admin roles. Retrieved from https://support.office.com/en-us/article/About-Office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d

Microsoft. (2017b). Azure Active Directory Pass-through Authentication: Current limitations. Retrieved from https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication-current-limitations

Microsoft. (2017c). Compliance Manager. Retrieved from https://servicetrust.microsoft.com/

Microsoft. (2017d). GDPR Trust Center. Retrieved from https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

Microsoft. (2017e). PowerShell for Office 365 administrators. Retrieved from https://support.office.com/en-us/article/PowerShell-for-Office-365-administrators-40fdcbd4-c34f-42ab-8678-8b3751137ef1

Microsoft. (2017f). Understanding Office 365 identity and Azure Active Directory. Retrieved from https://support.office.com/en-us/article/Understanding-Office-365-identity-and-Azure-Active-Directory-06a189e7-5ec6-4af2-94bf-a22ea225a7a9

Microsoft. (2017g). What is Office 365. Retrieved from https://products.office.com/en-us/

Skyhigh. (2016). *Office 365 Adoption & Risk Report* (pp. 14). Retrieved from https://info.skyhighnetworks.com/rs/274-AUP-214/images/Skyhigh%20O365%20Report%20Q2%202016.pdf

Syynimaa, N. (2017). Security vulnerability in Azure AD & Office 365 identity federation. Retrieved from http://o365blog.com/post/federation-vulnerability/

Tomisek, J. (2015). Office 365 v. Google Apps: A data protection perspective. *Masaryk UJL & Tech., 9*, 85.