



APPLYING THE TRAFFIC LIGHT PROTOCOL TO PURVIEW INFORMATION PROTECTION

A Simple Guide

What is this?

This guide will walk through the basics of implementing Purview Information Protection following the Traffic Light Protocol (TLP)

This content is provided **as is** with no warranty whether express or implied. Every organization and person should make their own educated decisions around cybersecurity implementations. Dom Kirby and Dom Kirby Creative accept no liability for your use of or reliance upon this content.

Dom Kirby
domkirby.com

TLP originates from [FIRST](#) (Forum of Incident Response and Security Teams). However, anyone can use TLP and it is widely used by federal agencies like [CISA](#) and information security organizations such as ISACs. Poke around on alerts from CISA or within Infragard (if you're a member) and you will often see TLP labels.

Throughout this guide, I'll be using CISA's description of TLP labels and other concepts. See <https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage>

Additionally, this guide covers TLP version 2.0, which is the authoritative revision as of writing.

Note: Purview markings will not achieve TLP markings to the published specification. I'm okay with this, but make sure you are too before relying on this methodology. You may want to apply your own markings on official communications in addition to Purview's markings.

First Thing's First: What is the TLP?

Before we dive into implementing the Traffic Light Protocol (TLP), it is important that you understand what the TLP is and who it is meant for. The TLP **is not** necessarily designed to be used as a mechanism to classify and protect *internal* sensitive information. Quite the contrary, it's meant to enable the safe sharing of information amongst organizations or groups of people.

The TLP is a widely used information sharing protocol or framework in the cybersecurity information sharing community. It is heavily used amongst ISACs, federal agencies, and other sharing organizations. The intent is simple: **provide absolute clarity around what you may do with information you receive from someone.** By standardizing on the TLP, organizations can share data with each other with a defined information sharing policy instead of having to use their own internal policies (leaving lots of room for confusion).

TLP's Goal Makes it the Wrong Choice for Internal Data

At the risk of over-repeating myself, **TLP is not meant to classify your organization's internal confidential information!** TLP should be used when sharing information, your organization's information labels should be leveraged for internal information not to be shared outside the walls. Internal information labeling is not within the scope of this document. Work with your information security team or MSP to learn more about implementing internal data classification.

TLP Labels/Levels

For simplicity, TLP is broken down into five levels (from least to most restrictive):

Level	Information may be Shared
TLP:CLEAR (f.k.a. TLP:WHITE)	Publicly
TLP:GREEN	Within the appropriately defined community.
TLP:AMBER	Within the recipient organization and its clients.
TLP:AMBER+STRICT	Within the recipient organization only.
TLP:RED	Recipient or parties to the conversation only (a party being the individual, it is effectively a secret

As you can see, TLP provides a simple expectation around what one can do with the information you send to them. The higher the color, the less permission you have to share content from CLEAR (public information) to RED (only shareable to the people involved in the conversation or communication).

To keep things simple, I like to align my descriptions to CISA's really simple one liners:

Level	Description
TLP:CLEAR (f.k.a. TLP:WHITE)	Disclosure is not limited.
TLP:GREEN	Limited disclosure, restricted to the community.
TLP:AMBER	Limited disclosure, restricted to participants' organization and its clients.
TLP:AMBER+STRICT	Limited disclosure, restricted to participants' organization.
TLP:RED	Not for disclosure, restricted to participants only.

What Information should I Protect with TLP?

The information to which you choose to apply TLP is entirely up to you. I'm writing this guide simply to share the general idea of TLP and how you could implement it within your own tenant. In my personal tenant, I don't do a lot of internal collaboration. But I do quite a bit of external collaboration involving sensitive information. I use TLP to mark what I want the recipient to do with it. You may apply TLP to entirely different types of information. The whole idea of TLP, even though it originated for cybersecurity information, is that it can be applied to just about any information sharing scenario.

I've shared a few of my own examples below, but you can also see it in all kinds of places by looking for "TLP:CLEAR" on Google. If you're an Infragard member, you're likely to see a fair amount of TLP:GREEN information (although since it is a federal program, you'll see lots of old school FOUO as well). I treat FOUO as red, although that often isn't the intent (this is why TLP is better).

Examples

1. If I'm sending content to Matt Lee about a vulnerability presentation we're going to do, that conversation is going to start at **TLP:RED**. We haven't yet decided how much we're going to publicly disclose, and we don't want everyone knowing the content yet. As we work into a publicly ready version, we'll eventually have content that is TLP:CLEAR or TLP:GREEN depending on the scope of our presentation.
2. If I am participating in an exchange of secrets with someone, I will apply TLP:RED to communicate that the information is for the eyes of the recipient and I only.
3. If I am working on a project that is not yet released, with a group of people from different orgs, I may apply AMBER or AMBER+STRICT to allow other teams to communicate information to the correct individuals.

Implied Levels

Among friends, there is also a concept of "implied" TLP levels. For example, most people I Signal with know that any conversation in Signal is TLP:RED unless one of us says otherwise about a specific message. **However**, implied levels **are not** a concept present in TLP as written and thus should only be relied upon amongst friends.

Enough History, Let's Implement

Okay, you know what TLP is. You want to use TLP. Let's use Purview Information Protection to implement Information Labeling/data classification in the TLP format. Before we dive in, let's cover some caveats:

- The TLP specification is very specific on **how** you are supposed to apply markings. The white on black, size 12 font TLP:CLEAR in the header of this document is a "proper" label for TLP clear. PIP will not allow you to mark content with this specific format. For me, I'm okay with that. However, if you're doing official work, you'll need to add manual markings in addition to Purview's.
- Also due to the picky specifications, we'll be a bit non-compliant in the names of our information protection labels. You can't use a ":" in a label's display name, so we'll have to replace that with a space. In our content markings, we can still use colons. External parties won't see your actual label names, just the markings they apply.
- Purview's label coloring options will not cover the specific colors called for by the TLP specifications. As such, we're taking liberties here.
- In general, remember that I'm just sharing an idea here. You can apply this (or not) however you wish.

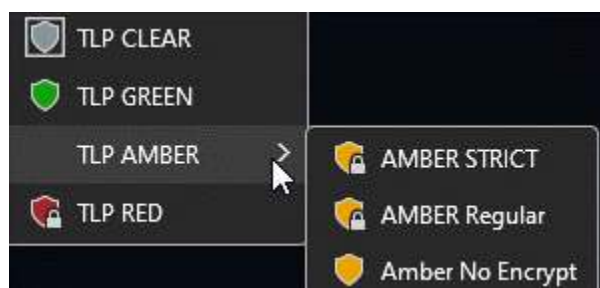
Licensing Requirements

Information labeling has certain license requirements from Microsoft. My example tenant is an E5 Developer's tenant, but these settings are available in Business Premium as well.

Purview Information Protection in General

Purview Information Protection is a complicated product and has a lot of functionality. If you're reading this guide, I'm assuming you already understand the concept of PIP and how it works. If you don't, please read up on it (<https://learn.microsoft.com/en-us/purview/information-protection>) before proceeding.

Label Architecture



In this document, I'll be nesting the TLP levels under a parent "TLP" level. This is based on the assumption that you already have other internal labels such as "Confidential" and will help keep things neat and tidy. In my own tenant, I actually have TLP at the parent level as shown in the example on the left. If you're working in your personal tenant, you may prefer my personal

tenant's approach since you're likely doing more external collaboration than internal collaboration.

In a company setting, I highly recommend the nested approach so that there is clear separation between internal classification labels and external (TLP) classification labels. Ultimately, you need to choose what works best for you and the people you're working with.

The Labels

We are going to build six labels in this deployment:

- ✓ **TLP/CLEAR**
- ✓ **TLP /GREEN**
- ✓ **TLP/AMBER NO ENCRYPT**
- ✓ **TLP/AMBER ENCRYPT** (*AMBER Regular in the above graphic*)
- ✓ **TLP/AMBER STRICT**
- ✓ **TLP/RED**

*These labels are intentionally ordered by sensitivity of the content **and** the impact the labels will have (increasing restrictions).*

You may choose to remove some or add some. You probably noticed the "TLP AMBER NO ENCRYPT" label. If TLP:AMBER data is sensitive, why wouldn't I encrypt it? The answer is that I typically would, **but** AMBER is relatively broad in its distribution. Sometimes applying encryption makes it difficult for someone to share that information within the defined bounds. In those scenarios, I may apply TLP:AMBER without encryption, but with the appropriate markings. TLP RED is **always** encrypted with "Do Not Forward" applied to email messages. TLP:RED information is expected to **never** be shared outside that conversation, so that is a fair encryption approach.


Let's Get Building

All of the building we're doing will be done within the confines of the Purview/Compliance portal at <https://compliance.microsoft.com>.

Building the Base TLP Label

First, we're going to build a base "TLP" label. This will allow us to list the TLP labels separately from other labels we may have like "Contoso Confidential." If you'd prefer to have your TLP labels be at the top level, skip this section and add "TLP" to the front of the name of each of the six sublabels.

This is a parent label. Once we add sublabels, you will not be able to select this label when classifying data.

1. In the Purview portal, navigate to "Information protection" → "Labels"
(<https://compliance.microsoft.com/informationprotection/labels>)
 Create a label
2. If you have any, you will see your existing labels listed here. Click
 - a. For the name, enter "TLP Parent Label" (this is an internal/administrative name, you don't see it on the user end)
 - b. For the Display name enter "TLP"
 - c. For the description, use something helpful such as "Apply a Traffic Light Protocol level to this content for external sharing." (You may want to add more about how this isn't for internal data etc.)
 - d. Enter whatever description you would like to see as an admin
 - e. Choose a color. **Note:** Unfortunately, when using nested labels, only the parent label color applies. As such, I would stay away from amber or red as the color. To

have uniquely colored labels, use top-level labels for TLP levels.

Name * ⓘ

Display name * ⓘ

Label priority ⓘ
 ⓘ By default, this label will be assigned the highest priority, but you can change this after it's created.

Description for users * ⓘ

Description for admins ⓘ

Label color ⓘ

3. Click Next
4. Set your Scope as you see fit. I'm using Files and Emails. Click Next.
5. Since this is just our parent label, we won't be doing any marking or encryption. Click Next.
6. We don't need auto labeling, click Next.
7. We're not using Groups and Sites, Click Next.
8. If asked about schematized data assets (preview), click Next.
9. Click Create label.
10. We **are not ready to publish** so click Don't create a policy and Done.

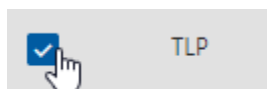
Don't create a policy yet
 You can publish or auto-apply this label later.

You should now be back to your list of labels.

TLP:CLEAR

TLP:CLEAR is the least restrictive TLP level (in fact, it's meant to mark information that can be shared with the general public). It will be the first one we create. Because we have a top label of "TLP," we will exclude "TLP" from our sublabels. This means our labeling of content will appear something like TLP/CLEAR when we select a classification (but our markings will be closer to spec).

1. Check the box next to your TLP label



+ Create sublabel

2. Click [button] at the top.
3. For the Name enter CLEAR (this is an internal name, you can add more content if you wish)
4. For Display name, also enter CLEAR.
5. I'll be using the CISA one-liners for label descriptions. As such, the Description for users will be "Disclosure is not limited."
6. If desired, input an admin description.
7. The color of the label is inherited from the parent (use top labels instead of nested labels if you wish to have unique internal colors)
8. Click Next.
9. Set your Scope as desired, I'm using Files and Emails.
10. Click Next.
11. Since this is public information, we will not apply encryption. However, we want to mark this information TLP:CLEAR, so we will apply content marking.

Apply or remove encryption
Control who can access item

Apply content marking
Add custom headers, footer:

12. Click Next.
13. Flip the switch for Content marking
 - a. Check header and Footer
 - b. Customize the Header
 - i. Header text: TLP:CLEAR
 - ii. Font size: 12 is the spec, I did 10 for cleanliness.
 - iii. Font color: Black
 - iv. Align text: Your call, I did left (remember we can't meet the TLP marking as specified in the documentation).
 - v. Click Save
 - c. Customize the Footer
 - i. Footer text: TLP:CLEAR - Disclosure is not limited.
 - ii. Font size: 12 is the spec, I did 10 for cleanliness.
 - iii. Font color: Black
 - iv. Align text: Your call, I did center
 - v. Click Save.
14. Click Next.
15. We are not enabling Auto-labeling; click Next.
16. We are not enabling Groups and Sites; click Next.
17. If presented, click Next for schematized data assets.

I opted to include the description of the label in the footer. This is optional but will help a recipient who isn't familiar with the TLP.

18. Click Create label.
19. Choose Don't create a policy and click Done.

You will be brought back to your labels list. You should now have your TLP label with CLEAR nested under it:

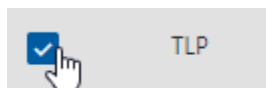


Now, when labeling content, the label will show as TLP/CLEAR internally but the label will apply “TLP:CLEAR” markings.

TLP:GREEN

TLP:GREEN is the second-least restrictive TLP level.

1. Check the box next to your TLP label



[+ Create sublabel](#)

2. Click [+ Create sublabel](#) at the top.
3. For the Name enter GREEN (this is an internal name, you can add more content if you wish)
4. For Display name, also enter GREEN.
5. I'll be using the CISA one-liners for label descriptions. As such, the Description for users will be “Limited disclosure, restricted to the community.”
6. If desired, input an admin description.
7. The color of the label is inherited from the parent (use top labels instead of nested labels if you wish to have unique internal colors)
8. Click Next.
9. Set your Scope as desired, I'm using Files and Emails.
10. Click Next.
11. Since this is lightly restricted information, we will not apply encryption (although you could choose to do so). However, we want to mark this information TLP:GREEN, so we will apply content marking.

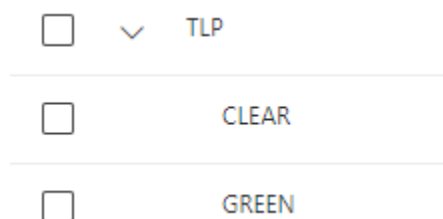
Apply or remove encryption
Control who can access item

Apply content marking
Add custom headers, footer:

12. Click Next.
13. Flip the switch for Content marking
 - a. Check header and Footer
 - b. Customize the Header

- i. Header text: TLP:GREEN
 - ii. Font size: 12 is the spec, I did 10 for cleanliness.
 - iii. Font color: Green
 - iv. Align text: Your call, I did left.
 - v. Click Save
 - c. Customize the Footer
 - i. Footer text: TLP:GREEN - Limited disclosure, restricted to the community.
 - ii. Font size: 12 is the spec, I did 10 for cleanliness.
 - iii. Font color: Green
 - iv. Align text: Your call, I did center
 - v. Click Save.
14. Click Next.
 15. We are not enabling Auto-labeling; click Next.
 16. We are not enabling Groups and Sites; click Next.
 17. If presented, click Next for schematized data assets.
 18. Click Create label.
 19. Choose Don't create a policy and click Done.

You're going to see a lot of the labels list throughout this process. Now we have both CLEAR and GREEN under TLP:



TLP:AMBER (No Encrypt)

We're making progress! At this point, this process will feel repetitive, because it is. By its nature, information marked **TLP:AMBER** is a little sensitive, so logic would dictate that we encrypt it. However, the distribution intent for AMBER can be broad (the recipient organization *and* their clients. I prefer to encrypt, but sometimes a marking will suffice when we need to ensure a trusted recipient's ability to disseminate information within the AMBER boundaries.

To save you a few bytes when you download this document, I'm going to shorten the process. Repeat the steps for TLP:GREEN but use the following information:

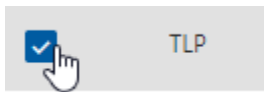
- Name: AMBER (No Encrypt)
- Display name: AMBER NO ENCRYPT
- Description for users: Limited disclosure, restricted to participants' organization and its clients. USE WITH CAUTION: Encryption no applied.
- Content marking:
 - Header: TLP:AMBER
 - Size: 12 is the spec, I did 10 for cleanliness.
 - Color: Yellow (or black if Yellow is tricky for you to read)

- Align text: Your call, I did left.
- Footer: TLP:AMBER - Limited disclosure, restricted to participants' organization and its clients.
 - Size: 12 is the spec, I did 10 for cleanliness.
 - Color: Yellow (or black if Yellow is tricky for you to read)
 - Align text: Your call, I did center.

TLP:AMBER (Encrypt) and TLP:AMBER+STRICT

AMBER ENCRYPT and AMBER+STRICT are nearly identical labels except for their name. As such, we'll simplify things here and include them both in one set of instructions. **Note:** AMBER ENCRYPT implies the same bounds as TLP:AMBER but applies encryption (it does not change your expected dissemination boundaries).

1. Check the box next to your TLP label



+ Create sublabel

2. Click [button] at the top.
3. For the Name enter AMBER (Encrypt) and then AMBER STRICT the next time around (this is an internal name, you can add more content if you wish)
4. For Display name, enter AMBER ENCRYPT and AMBER STRICT the second time around.
5. I'll be using the CISA one-liners for label descriptions. As such, the Description for users will be:

AMBER ENCRYPT	AMBER STRICT
Limited disclosure, restricted to participants' organization and its clients.	Limited disclosure, restricted to participants' organization.

6. If desired, input an admin description.
7. The color of the label is inherited from the parent (use top labels instead of nested labels if you wish to have unique internal colors)
8. Click Next.
9. Set your Scope as desired, I'm using Files and Emails.
10. Click Next.
11. We're moving to higher levels of sensitivity here, so we **will** be encrypting **and** marking the content.

Apply or remove encryption
Control who can access items that have this label applied.

Apply content marking
Add custom headers, footers, and watermarks to items that

12. Click Next.

13. You will be brought to the encryption settings. Choose the following options:
 - a. Configure encryption settings.
 - b. Let users assign permissions when they apply the label. (Since this is meant to be shared externally, we can't really apply group restrictions like we would with internal labeling)
 - c. Check "In Outlook, enforce one of the following restrictions."
 - i. Choose "Encrypt-Only" (AMBER information is meant to be shared within approved boundaries, Do Not Forward would prevent this).
 - d. Check In Word, PowerPoint, and Excel, prompt users to specify permissions. This will cause a prompt to appear when this label is applied to a document, and users will specify who can read the document. **This** is what makes encryption tricky for dissemination of AMBER information.
14. Click Next
15. Flip the switch for Content marking
 - a. Check header and Footer
 - b. Customize the Header

AMBER ENCRYPT	AMBER STRICT
<ul style="list-style-type: none"> • Header text: TLP:AMBER • Font size: 12 is the spec, I did 10 for cleanliness. • Font color: Yellow • Align text: Your call, I did left. • Click Save 	<ul style="list-style-type: none"> • Header text: TLP:AMBER+STRICT • Font size: 12 is the spec, I did 10 for cleanliness. • Font color: Yellow • Align text: Your call, I did left. • Click Save

- c. Customize the Footer

AMBER ENCRYPT	AMBER STRICT
<ul style="list-style-type: none"> • Footer text: TLP:AMBER - Limited disclosure, restricted to participants' organization and its clients. • Font size: 12 is the spec, I did 10 for cleanliness. • Font color: Yellow • Align text: Your call, I did center. • Click Save. 	<ul style="list-style-type: none"> • Footer text: TLP:AMBER+STRICT - Limited disclosure, restricted to participants' organization. • Font size: 12 is the spec, I did 10 for cleanliness. • Font color: Yellow • Align text: Your call, I did center. • Click Save.

16. Click Next.
17. We are not enabling Auto-labeling; click Next.
18. We are not enabling Groups and Sites; click Next.
19. If presented, click Next for schematized data assets.
20. Click Create label.

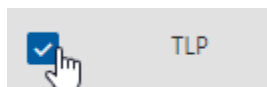
21. Choose Don't create a policy and click Done.

Almost there!

TLP:RED

TLP:RED is the **most restrictive** TLP level for sharing data. It sets the expectation that **only the people involved in the conversation** may use the information. If somebody sends you something with a TLP:RED marking, they mean to say that the information is for you and you only (or better described, only the people on that conversation). You should never share this information outside of the small group of involved insiders.

1. Check the box next to your TLP label



+ Create sublabel

2. Click TLP at the top.
3. For the Name enter RED (this is an internal name, you can add more content if you wish)
4. For Display name, enter RED.
5. I'll be using the CISA one-liners for label descriptions. As such, the Description for users will be: Not for disclosure, restricted to participants only.
6. If desired, input an admin description.
7. The color of the label is inherited from the parent (use top labels instead of nested labels if you wish to have unique internal colors)
8. Click Next.
9. Set your Scope as desired, I'm using Files and Emails.
10. Click Next.
11. We're moving to higher levels of sensitivity here, so we **will** be encrypting **and** marking the content.

Apply or remove encryption

Control who can access items that have this label applied.

Apply content marking

Add custom headers, footers, and watermarks to items that

12. Click Next.

13. You will be brought to the encryption settings. Choose the following options:

- a. Configure encryption settings.
- b. Let users assign permissions when they apply the label. (Since this is meant to be shared externally, we can't really apply group restrictions like we would with internal labeling)
- c. Check "In Outlook, enforce one of the following restrictions."
 - i. Choose "Do Not Forward" – This will mark emails as "Do Not Forward" and remove forwarding capabilities (this also prevents a recipient from creating new access rights on the thread).

- d. Check In Word, PowerPoint, and Excel, prompt users to specify permissions. This will cause a prompt to appear when this label is applied to a document, and users will specify who can read the document.

14. Click Next

15. Flip the switch for Content marking

- a. Check header and Footer
- b. Customize the Header

RED
<ul style="list-style-type: none">• Header text: TLP:RED• Font size: I used 12 here because this label should be big and annoying• Font color: Red• Align text: Your call, I did left.• Click Save

- c. Customize the Footer

RED
<ul style="list-style-type: none">• Footer text: TLP:RED - Limited disclosure, restricted to participants' organization and its clients.• Font size: I used 12 here because this label should be big and annoying.• Font color: Red• Align text: Your call, I did center.• Click Save. <p><i>You may wish to apply something a little more aggressive to the RED footer to make it clear that this information isn't to be shared. It's up to you.</i></p>

16. Click Next.

17. We are not enabling Auto-labeling; click Next.

18. We are not enabling Groups and Sites; click Next.

19. If presented, click Next for schematized data assets.

20. Click Create label.

21. Choose Don't create a policy and click Done.

That's all the labels! If we did everything correctly, we should now have the following nested under our TLP label:

▼ TLP
CLEAR
GREEN
AMBER NO ENCRYPT
AMBER ENCRYPT
AMBER STRICT
RED

Rolling it Out

Now that you've got all of these different labels to work with, we need to publish them. I'm assuming that you have a baseline knowledge of Purview Information Protection, so I'm not going to go through the entire label policy process. The PIP docs are available here:

<https://learn.microsoft.com/en-us/purview/information-protection>. If this is your first time here, brush up on the docs and get real familiar with the product before you go pushing policies. I will however give you some tips.

Label Priority

By default, all of these new labels will have the highest priority. Under the TLP label, you should leave CLEAR through RED in the same order. You may, however, wish to move the TLP label above some of your internally confidential labels. Otherwise, you're telling Purview that TLP:CLEAR is less sensitive than "Super Secret Finance Label" or whatever labels you have. Here's an example (using Microsoft's dev tenant pre-built labels):

<input type="checkbox"/>	☰	Name	Priority
<input type="checkbox"/>		Personal	⋮ 0 - lowest
<input type="checkbox"/>		Public	⋮ 1
<input type="checkbox"/>	>	TLP	⋮ 2
<input type="checkbox"/>	>	General	⋮ 9
<input type="checkbox"/>	>	Confidential	⋮ 12
<input type="checkbox"/>	>	Highly Confidential	⋮ 16

Placed between "Public" and internal data labels.

In the above example, TLP is set as higher priority (more sensitive) than “Public” but *less sensitive* than the classification labels for Contoso’s internally confidential data.

Policy Considerations

If you’re rolling this into an existing set of label policies, consider making TLP it’s own policy and only rolling it out to people who need to use the TLP (such as security researchers or people who collaborate with other orgs regarding sensitive data). **Be sure to look at your existing security policies (the paper ones). Chances are, they do not account for using the TLP and thus you will need to write it in.**

That’s It!

I hope this helps or at least satisfies some nerdy curiosity. It’s important to note that the Traffic Light Protocol was specifically designed to set standards around secure *sharing of information*. While you *could* implement a version of TLP for internal data, I would recommend a different methodology there to better align to role or department based access control.

All of that said, if you find yourself frequently working with others using sensitive data, the TLP is a great way to establish ground rules for dissemination of information based on an easy to share and train standard that also benefits from wide adoption and thus great documentation.

Applying the Traffic Light Protocol to Purview Information Protection © 2024 by [Dom Kirby / Dom Kirby Creative](#) is licensed under [CC BY-SA 4.0](#)