2021 EMAIL DELIVERABILITY GUIDE

Secrets for Better Inbox Placement

Contents

Definitions

What is spam?

Unsolicited
promotion

Spam (the unofficial name for UBE = unsolicited bulk email) refers to bulk emails or advertisement emails that are disseminated throughout the internet. They end up unsolicitedly in millions of electronic inboxes. Most spam emails are commercially motivated and are categorized as follows:

- Commercial email spam
- Chain letters, virus warnings, hoaxes
- Emails sent by viruses
- Phishing emails

Delivery (delivery rate)

Bounce handling
required

The delivery rate is the percentage of successfully sent emails (defined as receipt of the email in the inbox of the recipient) compared to the total number of emails sent. Bounces, meaning undeliverable emails, are not included. The delivery rate is, among other things, an indicator of the quality of the distribution list.
To keep the delivery rate constantly high, a process known as bounce handling is required, as implemented in Retarus' Global Suppression solution. Email addresses that cannot be delivered to are automatically removed from the distribution list.

Reputation / sender score

The higher,
the better

Scores are calculated as a moving average over a period of 30 days and represent the ranking of an IP address compared to other IP addresses. It is similar to a percentile rank. The closer to 0 the score is, the worse it is. The closer to 100 the score is, the more effective the sender.

Complaints: This is calculated by dividing the number of complaints by the number of received emails. It also considers the number of complaints the IP address receives compared to other IPs.

Volume: The sheer dispatch volume is not an indicator of whether a sender has a good or bad reputation. However, it is an important part of the general algorithm. For example, an IP address that sends 100 emails and receives 99 complaints is ranked as questionable. In contrast, an IP address that sends 100,000 emails and receives 99 complaints is ranked as having a good reputation. Thus, the volume always depends on other index values.

External reputation: This number indicates how a sender's IP address compares with other IP addresses also listed on numerous external blacklists and whitelists.

Unknown contacts: The ratio of an IP address' unknown contacts to other addresses is taken directly from the incoming SMTP logins of the involved ISPs. It measures how often an IP address attempts to send an email to a recipient that does not exist.

Rejected emails: This measures how often sent emails result in a soft or hard bounce as compared to other IP addresses.

Accepted emails: This number represents how many emails are accepted by the ISPs and forwarded to the recipients. The number is comprised of all sent emails minus the number of rejected emails.

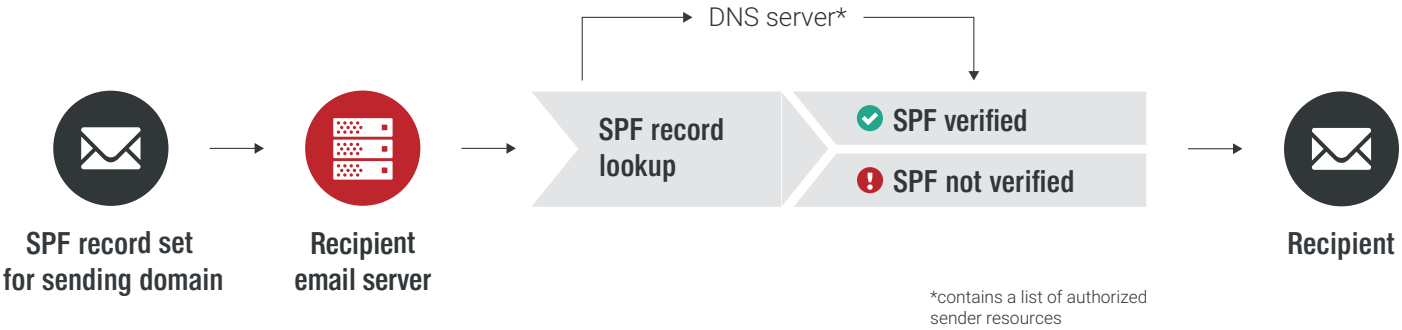
Ratio of accepted emails: The number of accepted emails compared to the total number of sent emails. To obtain this ratio, the number of read emails is divided by number of sent emails.

Ratio of unknown contacts: The number of unknown contacts or invalid email addresses is compared to the number of sent emails.

SPF record

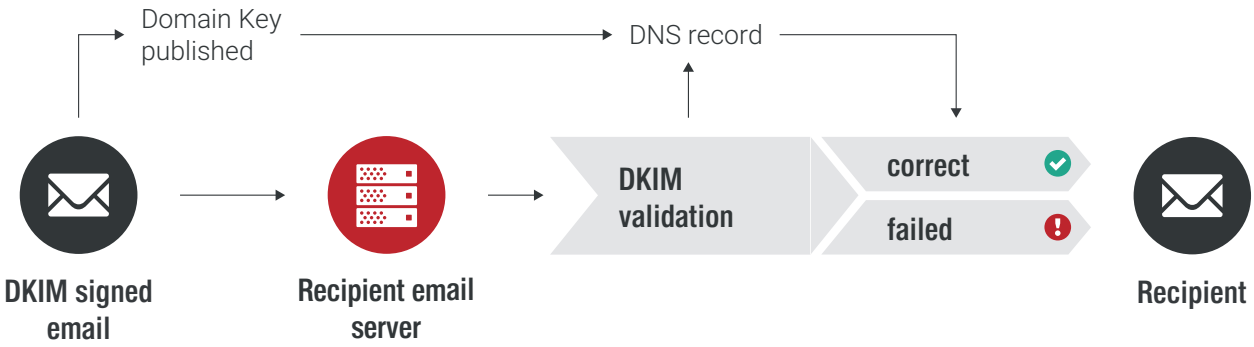
Sender in
DNS

The Sender Policy Framework (SPF), formerly known as Sender Permitted From, is a method designed to prevent the falsification of email sender addresses. It was created as a way to prevent spam. SPF is a record in which the owner of a domain listed in the Domain Name System specifies which computers are allowed to send emails for this very domain.
The administrator of a domain saves a TXT resource record (RFC 7208 has rendered the SPF resource record obsolete) in the DNS zone. These resource records contain the IP addresses of the mail transfer agents (MTA) that are permitted to send emails for that particular domain. Using the domain specified in the "MAIL FROM" and "HELO" fields, the recipient verifies whether the sender is authorized to send the email. The recipient calls up the SPF information via the Domain Name System for the specified domain and compares the IP address of the sending MTA with the permitted addresses. If the IP addresses match, the sender is authentic. If not, the email can be discarded.



DKIM

DomainKeys is a protocol to ensure the authenticity of email senders. It was designed to help prevent and stop unwanted emails such as spam or phishing attempts. DomainKeys are based on asymmetric encryption. The email is given a digital signature that the recipient server can verify using the public key, which is available in the Domain Name System (DNS) of the domain. If verification fails, the recipient mail transfer agent (MTA) or the recipient application can refuse or sort out the email.



DMARC

SPF + DKIM =
Policies

DMARC – short for Domain-based Message Authentication, Reporting, and Conformance – is a complementary technical specification designed to protect email senders and recipients from spam, spoofing, and phishing.
With DMARC, the sender can specify guidelines on how the receiving servers should handle email authentication. DMARC itself is not an independent protocol, but builds on the SPF and DKIM standards mentioned above. The DMARC policies for accepting emails are published by the domain administrator as part of the DNS records of the respective domain.
When an incoming mail server supports DMARC and receives an email, it accesses the DNS record to "look up" the policy stored there for the domain contained in the "From" header (RFC 5322). In addition to matching the DKIM signature, it checks whether the message originates from an IP address that is allowed in the SPF records of the sending domain.
After the DMARC policy has been applied, the receiving mail server reports the result to the owner of the sending domain. Any misuse of the sending domain is reported as well.

BIMI

Show the flag
with your logo

BIMI is the acronym for Brand Indicators for Message Identification. It is a fairly new open standard for mailbox providers (MBPs) that was jointly developed by several large companies such as Google, Microsoft, Yahoo and PayPal. Email senders can use BIMI to display the well-known brand or company logo as a graphic next to the sender's name to indicate a professional and reputable sender to email recipients.
BIMI is an open standard that basically any sender can use. It is based on the already established standards SPF, DKIM, and DMARC. If these have been successfully implemented, then BIMI can be set up with correspondingly little effort:

- The DMARC policy must be set to "Reject" and/or "Quarantine".
- The desired logo should be a square graphic without text in SVG Tiny PS format at a freely accessible web address.
- Within the DNS entry, a TXT record has to be created for the respective "From" address: `default.bimi.[domain] IN TXT "v=BIMI1; l=[SVG URL]; a=[PEM URL]`

Further information can be found at bimigroup.org.

Other definitions in the transactional world of email

Inbox placement rate: Deliverability rate minus the number of emails that have ended up in the spam or junk email folder

Soft bounces: Emails that are sent to existing addresses but cannot be delivered temporarily (e.g. because of an out-of-office reply)

Hard bounces: Emails that cannot be delivered permanently (recipient has left the company, etc.)

Open rate: Number of openings divided by the number of delivered emails

Unique click rate: Number of clicks in an email (excluding multiple clicks by a user) divided by the number of emails delivered.

Total click rate: Number of all clicks in an email divided by the number of delivered emails

Click to open rate: Unique click rate divided by the opening rate

Conversion rate: The number of targeted actions divided by the effective click rate

Bounce rate: The number of bounces divided by the number of delivered emails

Risks and pitfalls

Doubly painful

A current study conducted by Return Path, an email intelligence company, determined that 20 percent of sent and desired emails do not reach their intended recipients. Undelivered emails hurt a company in two ways:

- Reduced reach of marketing campaigns leads to direct revenue losses. The revenue potential that ends up in German spam folders alone each year is estimated at around 3 billion euros.
- Yet companies incur more than just financial loss when emails are mistakenly classified as spam. The reputation of the company or brand also suffers when sender addresses appear on blacklists and the company receives a negative rating as an email sender.

Causes of spam classification

The reasons for being classified as spam can be manifold: spam traps, cold IPs, the design of the email, and reputation scores. It is reasonable that users want to protect their email inbox and computer from internet-based attacks using security software. Such need for security on the part of customers should be taken into account when planning email marketing activities.

	BLACKLIST	GREYLIST
Definition	• Directory of IP addresses and domains that are classified as negative because they send unwanted emails • Emails sent via this IP get intercepted / blocked • Large email providers typically use multiple blacklist providers	• Rejection of an unknown email address and / or IP address on the first attempt at delivery • A subsequent second attempt is usually successful
Advantages	• Protects the user from undesired communication	• Effective spam prevention: Many spammers give up after the first attempt. Real email servers typically try to deliver a second time. • After successful email delivery, the combination of sender, recipient, and email server is entered into the whitelist and subsequent emails are delivered.
Disadvantages	• Desired emails on the blacklist, e.g. when a whole domain is blocked although only a subdomain sends spam • Revenue loss and image damage for the sender – campaigns sent via a blacklisted IP are not delivered • Cumbersome delisting. It is possible to be removed from a blacklist if you accidentally end up on it. In case of multiple violations, however, senders may get permanently blacklisted • Unfair business model	• With greylisting, a desirable email can be delivered a few minutes or even a hours later • As soon as the first attempt is made, some email servers generate a temporary delivery report for the sender, which might be interpreted as failed delivery in some cases

International peculiarities

The saying "different countries, different customs" also applies to email marketing, where there is a multitude of national regulations and peculiarities to understand. Failure to comply with these can result in heavy fines or even criminal sanctions.

USA – CAN SPAM Act (2003)

The federal mandate Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), passed in 2003, prohibits the sending of Commercial Electronic Messages (CEMs) – unless they meet the following requirements:

Content

- The commercial nature of the email must be clear (unless consent has been obtained in advance).
- The email must have a proper header.
- The subject line must be relevant to the offer in the body of the message.
- Adult content must be marked separately (label).
- The email must contain a valid physical address of the sender.
- The email must contain a cancellation option that will be processed within 10 days ("opt-out").

Commercial nature
must be clear

You may contact individuals or companies without prior consent as long as you adhere to the above requirements and do not use unlawful means to collect email addresses. An example of unlawful means is the use of an automated email generator.
In the event of a breach, fines can be up to $16,000 per breach, per email.

European Union – GDPR

Market place
principle

Due to its nature, the General Data Protection Regulation (GDPR) is legally binding in all countries and has had direct legal effect since May 25, 2018.
The regulation applies to all individuals and companies in the EU. Regardless of where the sender is based, anyone who acquires email addresses and sends emails to recipients in the EU is covered by the law.

Design of the email

- Every email sent must contain an easily recognizable imprint that complies with the applicable legal requirements.

The following also applies to the sending of emails with advertising content:

- The client of an advertising mailing must be clearly identifiable.
- In each email, the recipient must be informed separately of their ability to revoke consent to the sender at any time. The revocation / unsubscription of emails (opt-out / unsubscribe) must be possible for the recipient without further ado, i.e. without entering access data such as login and password.
- In the header and subject line of the email, neither the sender nor the commercial character of the message may be concealed or hidden. Obfuscation or concealment means that the header and subject line are intentionally designed so that the recipient receives no or misleading information about the actual identity of the sender or the commercial nature of the message before viewing the content of the communication.

Technical configuration

- Sender addresses are subject to registration and are part of the service administration. The sender address must be able to receive emails (valid MX record). The sender domain must also have a valid DNS-A record. Role-based sender addresses (e.g. abuse@), postmaster@) are not permitted.
- The customer must remove email addresses from the relevant distribution lists immediately if they are detected as non-existent after sending, but no later than after three hard bounces. Overall, the hard bounce rate per ISP must not exceed 1.0 percent. Role-based recipient addresses (e.g., postmaster@, abuse@) are discarded.
- The customer must remove email addresses from the relevant distribution lists if the recipient classifies the email as spam and reports this (complaint) or revokes their consent to the sender.

The regulation also applies retroactively. If you cannot prove the consent of your current recipients, you may no longer send them emails.
The GDPR not only standardizes the requirements, but also the penalties. Violations can cost companies a maximum of 4 percent of their annual global turnover or EUR 20 million, whichever is greater.

Be careful with sensitive topics

China

China's anti-spam legislation is defined by the Measures for the Administration of Internet Email Services (2006) and the Consumer Rights Protection Law (2013). It applies to all emails sent to citizens of China and people who receive email while in China. The requirements for lawful email are as follows:

- Explicit consent is required (opt-in approach).
- Authorization must be verifiable and recorded for audit purposes.
- The commercial nature of the email must be clear.
- The subject line must contain the word "ad" or "advertisement" in English or Chinese.
- The identity or origin of the sender must not be intentionally concealed or falsified.
- The email must contain valid contact methods, including the sender's email address. Recipients may then send their refusal to receive further emails, which must be valid for 30 days.

Content

- Any message of a promotional nature falls under this regulation.
- For any external link in an email there must be a written guarantee that the message does not contain spyware (the situation for images / thumbnails is unclear).

Special restrictions apply to content in China. These are vaguely defined in Article 57 of the Telecommunications Ordinance. Obvious examples are politically sensitive topics, but also anything considered obscene.

Fines range from CNY 10,000 to CNY 30,000 per email. Despite strict regulations and high fines, there has been no notable verdict so far. Therefore, spam remains a major problem in China.

In any case, before you decide on email marketing activities in China, you should check the very dynamic list of keywords on the local authorities' blacklist.

Guidelines for good deliverability

Deliverability is one of the most important keys to professional email marketing. The quality of the systems used by companies to send email campaigns is important. They must be able to maintain high deliverability rates and be expandable.

Warming up unknown IPs

Pre-glow
ignites better

The reputation of IP addresses is primarily based on historical sending patterns and volumes. An IP address that sends consistent volumes of emails over a long period of time typically means it is highly reputable. Companies that use dedicated IP addresses maintain their reputation as a sender by sending consistent and predictable volumes of emails.
Therefore, Retarus recommends the following when warming up a dedicated and yet unknown IP address:

- Duration of warm-up process: 6–8 weeks
- Start by sending a low volume of emails:
  - » Max. 1,000 emails on day 1
  - » Double the volume based on the previous day
  - » Start with throttled sending speed
  - » Slowly increase the volume, number of recipients, dispatch speed
- Cleanup the user list in parallel
- Use all available IPs and domains regularly so they remain known and are considered trustworthy
- Do not implement a sudden and extreme ramp-up
- Keep the risk of blacklisting as low as possible (beware of spam traps and affiliate campaigns)
- During the warm-up, dispatch attractive campaigns, not strategically important ones
- Focus the initial dispatch on particularly active and interested customers

Importance of "Shared IP" vs. "Dedicated IP"

A lot and often?
Own IP!

The more you look into high-volume emailing, the more you'll see the central importance of two different types of IP addresses:
Shared IP: Multiple senders share the same IP address.
Dedicated IP: One sender uses and is responsible for one IP address exclusively

Your goals as an email sender are part of the determination of whether you need a dedicated or shared IP address. You should consider indicators such as sending volume, frequency, as well as the quality of your mailing lists when making your decision.
If you are consistently sending high-volume campaigns or transactional messages, a dedicated IP address is recommended. You are the only party responsible for your reputation and protected from improper use by third parties.
If you send your campaigns or transactional emails on a smaller scale or more irregularly, a shared IP address is advisable. In this case you benefit from the activity of the additional senders to build and maintain the reputation of the IP.

Delivery rate

It is best to
document consent

Subscription using the double opt-in (DOI) method improves the quality of the distribution list. Only recipients who have chosen to register and whose email address exists receive emails.
DOI is a two-step process in which consent is given in the first step, followed by confirmation in the second – usually by activating a confirmation link. This prevents incorrect or third-party contact data from being entered improperly during registration.
For adequate proof, the DOI procedure must be properly logged, and the confirmation email has to somehow refer to the consent given. You should also double-check the respective local legal requirements (e.g., imprint obligation) in your jurisdiction.

CSA vouches for
quality

To increase the delivery rate even further, the recipient of the newsletter can be asked to add the sender to his personal address book or personal whitelist after registering for the newsletter. This is because desired emails and newsletters are often flagged as spam in the inbox of the subscriber ("false positives"). Participating in the Certified Senders Alliance (CSA), a central whitelist database requiring additional security measures, can also have a positive impact on the delivery rate.

Reputation

Binding screws
for your sender score

Since it takes a while to improve a poor sender score, senders should be aware of their reputation with the first email they send. There are several adjusting screws in email marketing that companies can review and adjust as needed to increase their sender score. The following factors have the greatest impact on email deliverability:

Fluctuating sending volume
Sending the same volume of emails consistently is crucial to a company's reputation. Peaks and other divergences can negatively impact the reputation.

Frequency of sent emails
Sending emails consistently has a positive effect on a company's reputation. It does not matter if a company sends emails daily, every other day, or every week. The frequency is based on marketing requirements. It is only important to ensure that emails are sent at regular intervals. Once a company's email marketing strategy is well designed and stable, tests can be used to determine the optimal frequency for each target group.

Being blacklisted
There are approximately 50 known blacklists recording spammer IPs. Retarus has added the largest and most popular blacklist operators to its active monitoring and keeps a watch on them. Should Retarus Transactional Email customers appear on one of these blacklists despite a warm-up and other measures designed to improve reputation, Retarus Customer Service will support the customer in delisting and will research the reason for the blacklisting. The results can help customers with improving their email marketing methods.

Spam traps
An email address that was once valid, but is now displayed to senders as a hard bounce. If a mail server registers that a sender regularly sends messages to an invalid address, this email address can be turned into a spam trap.
Senders then no longer receive a hard bounce notification, but the corresponding message is accepted, and its sender is marked as a spammer. Hence, one should keep an eye on hard bounces and maintain one's mailing lists regularly.

Spam reports
Recipients that categorize a sender as a spammer can report them in spam reports. This hurts the reputation of the sender.
Therefore, the latter should regularly check how high their spam quota is. Here's an indicator: there is no need to worry if one out of 1,000 emails is flagged as spam.

The distribution list
matters

Quality of the user list

The subscribe and unsubscribe function is now a matter of course in customer-friendly, reputable emailing. One reason for this is the legal framework for sending electronic mail. Sending newsletters is only legal if the recipient has given consent. Whitelist participants must give their consent with source and timestamp.

The unsubscribe function also plays an important role. A customer who can quickly and easily cancel a subscription will not report the email as spam. Important: If a customer unsubscribes from the mailing list, his address should be removed from the mailing list as soon as possible and by no means be written to again.

Using attachments

ISPs often check for potentially dangerous file types. These include, in particular, executable files (.exe) or scripts.

.ade	.js	msh	.ps1xml
.adp	.jse	.msh1	.ps2
.app	.ksh	.msh2	.ps2xml
.asp	.lib	.mshxml	.psc1
.bas	.lnk	.msh1xml	.psc2
.bat	.mad	.msh2xml	.tmp
.cer	.maf	.msi	.url
.chm	.mag	.msp	.vb
.cmd	.mam	.mst	.vbe
.com	.maq	.ops	.vbs
.cpl	.mar	.pcd	.vps
.crt	.mas	.pif	.vsmacros
csh	.mat	.plg	.vss
.der	.mau	.prf	.vst
.exe	.mav	.prg	.vsw
.fxp	.maw	.reg	.vxd
.gadget	.mda	.scf	.ws
.hlp	.mdb	.scr	.wsc
.hta	.mde	.sct	.wsf
.inf	.mdt	.shb	.wsh
.ins	.mdw	.shs	.xnk
.isp	.mdz	.sys	
.its	.msc	.ps1	

Role-based sender addresses

Role-based addresses ("function mailboxes") are usually company addresses that are not defined by a person, but by a job, and are often managed by several people or not monitored at all. Some of these address types are associated with high bounce rates and spam complaints. Therefore, they are blocked by Retarus upon request. In addition, role-based email addresses may not be used to register an account.

abuse@	list@	spam@
admin@	noc@	support@
billing@	no-reply@	sysadmin@
compliance@	noreply@	tech@
devnull@	null@	undisclosed-recipients@
dns@	phish@	unsubscribe@
ftp@	phishing@	usenet@
hostmaster@	postmaster@	uucp@
inoc@	privacy@	webmaster@
ispfeedback@	registrar@	www@
ispsupport@	root@	
list-request@	security@	

Strategy and prioritization of campaigns

The right strategy and proper prioritization of campaigns also contribute to maintaining a good reputation. The key to maintaining your reputation includes the following:

Defining the frequency

The time and frequency of sending campaign emails have a significant impact on how recipients categorize the emails. A flood of individual emails within just a few hours will most likely lead to rejection by the recipient. If this feedback impacts the ISP, it negatively affects the reputation.

Prioritization / addressing targeted groups

It is advisable not to send important mailings at the same time as less important campaigns. The increased volume of mailings increases the risk of negatively influencing the reputation. This reduces the delivery rate of the important campaigns, and the set target is not achieved.

Use differentiated communication channels with clear separation

Separate channels help achieve high delivery rates for campaigns. Campaigns should not be sent from the main domain, but rather from subdomains. Using dedicated IP addresses is even better.

Email content

The sender may neither disguise nor conceal the commercial nature of emails in the header and subject line of the email. An email is considered disguised or concealed if the header and subject line are presented so that the recipient is given no or misleading information about the actual identity of the sender or the commercial nature of the email before viewing its content.
Each email sent must contain an easily recognizable imprint that complies with the applicable statutory requirements.

Subject line

- Should always be present
- Short, but meaningful
- No capitalization or special characters
- No spam-suspicious terms (sex, free, ...)
- Appropriate to the content of the email
- No word repetitions

Tips for optimal email design

Ensure the relevance for the recipient is clear

Focus on a specific topic and present it clearly.

Use the above-the-fold space

Place the most important elements of the email at the very top so that they are spotted immediately.

Add appropriate calls to action

Make it clear to the reader what they should do and what they will get in return.

Give images a file name

Give images a suitable file name so that the reader understands its contents if it does not load.

Avoid spam terms

Do not use terms that have anything to do with money or prizes. This will ensure your newsletters land in the recipient's inbox and are not flagged as spam.

Enable social media sharing

Include share functions so that the reader can redistribute the newsletter.

Personalize the email

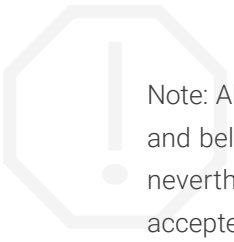
Recipients feel directly addressed when they read their own names. Therefore, address the recipient by name.

Furthermore, the following applies to the dispatch of emails containing promotional content

The initiator of a promotional email must be clearly recognizable and visible. Each email recipient must be made aware of the option to unsubscribe or opt out from receiving emails at any time. Opting out / unsubscribing from emails must, in general, be easy to do (logging in should not be required, for example).

We would be happy to explain to you in person how you can achieve deliverability with Retarus Transactional Email:

www.retarus.com/contact



Note: All information in this guide was researched to the best of our knowledge and belief and reflects the status at the time of creation. It is pointed out that nevertheless no liability for accuracy, timeliness and completeness can be accepted. This document does not replace legal advice in individual cases.

Authored by Retarus, as of June 2021.