CASE HANDBOOK:

HOW TO PREVENT SLAPPS OR GET HELP IF IT'S TOO LATE

June 2024

Table of Contents

Introduction

Welcome to the CASE anti-SLAPP Guidebook. This resource is meant to support smaller 'public watchdogs' (such as NGOs, media outlets or individual authors) that don't have access to a legal department.

Since you accessed this resource, you probably know what a SLAPP is, but if not, you can read more here. Briefly put, a SLAPP is a lawsuit issued to silence criticism, rather than obtain justice for an actual wrong. SLAPPs are a growing problem in Europe.

If you are investigating and publishing on the rich and powerful, SLAPPs are a danger you can't completely avoid. This Guidebook explains how you can make yourself less vulnerable to being sued, or else at least position your defence better. It also explains how to get help if you are facing a threat or an actual suit. The Guidebook covers the areas that are likely to be most relevant for readers: defamation, protest, copyright and trademark, whistleblowing, commercial and official secrets, and data protection law.

Each country in Europe has its own legal system (if not several). The general part of the Guidebook is based on common standards (deriving from the European Convention on Human Rights and EU law), and on what is "typical" in the legislation of European countries. There are also country-specific notes which help alert you to specific features of individual countries' laws, where we have that information available.

The best precaution is always to ask a qualified local lawyer in your jurisdiction for advice. This Guidebook is meant as the next best option. It is *not* legal advice and CASE makes every possible disclaimer of its legal liability in case you rely on the Guidebook. We hope you find it useful anyway.

The Guidebook was developed by a team drawn from member organisations of the Coalition Against SLAPPs in Europe (CASE), and peer-reviewed by lawyers whose job is to keep public watchdog organisations safe from SLAPPs. For feedback or questions, please write to contact@the-case.eu.

Preventing trouble with defamation law

Introduction

This section deals with defamation. Other words used that relate to defamation include libel, slander and calumny. Research done by the Coalition Against SLAPPs in Europe (CASE) shows that defamation is by far the most common legal ground on which public watchdogs are sued in Europe. Therefore it is useful to understand what constitutes defamation, and which steps one can take to prevent a lawsuit, or at least be in a strong position if one is sued.

Defamation law: the basics

What is defamation?

There is no Europe-wide definition of defamation but national laws are usually similar, and in most countries, you would be committing defamation if each of these conditions are met cumulatively:

1. You made a statement in public or to a third party (in any form: in an article, book, social media posting, interview etc.)
2. The statement caused harm, or could cause harm, to the reputation of another natural or legal person.
3. The statement was false or misleading.

Example

If you make a statement in public which harms someone's reputation, but it is true, you would not be liable for defamation. Nor would you be liable for defamation if you make a statement which is false but doesn't harm anyone's reputation.

What are the legal consequences of committing defamation?

You may be sued in a civil court for defamation and, if you lose, ordered to pay compensation for the damages caused, both economic losses (such as loss of income) and non-economic losses (such as loss of reputation and humiliation). The more people have seen or heard the defamatory statement, the greater the damages may be.

Courts in many countries can also order alternative or additional remedies, such as ordering you to publish a correction.

In many European countries, defamation is also a criminal offence, meaning that the victim could report you to the authorities, and a public prosecutor might then decide to bring criminal charges against you. In a smaller number of countries, victims can initiate prosecution in a criminal court themselves without having to rely on a public prosecutor. This is known as a 'private prosecution'.

Prison sentences for defamation are fortunately rare in practice.

Who is at risk of being sued?
In most countries, anyone can sue another person whom they consider responsible for the defamatory statement, such as the (co-)author, the entity that published the statement, or the person responsible within the entity for approving the publication, such as an editor-in-chief, in the case of a media outlet. In SLAPPs, it is quite common that an individual author is sued along with their employer, to increase the intimidatory effect.

Who can bring a defamation suit?
Defamation suits can be brought by private individuals or legal entities, such as companies or NGOs. In some countries, public bodies can sue for defamation too, although it is quite rare for them to do so.

As discussed above, criminal defamation cases can be brought by prosecutors or, in some countries, by private parties in a so-called private prosecution.

The European Court of Human Rights has established a strong principle that the limits of acceptable criticism are wider when speaking about persons or entities who have consciously entered the arena of public debate, or who wield significant influence. This for example includes politicians, public officials, public figures, public bodies and large corporations.

As a rule, the more power they yield and the more attention they draw to themselves, the higher the degree of tolerance they should display. This doesn't guarantee they *won't* sue - but they should have a harder time winning their case.

Can you commit defamation online?
Yes, defamation law usually applies regardless of the form and medium, so you can be sued for online statements, such as social media postings, comments, reviews and so on. The question of whether you can be held liable for hyperlinking, embedding etc. is discussed below.

In a cross-border situation, where can the defamation suit be brought and which country's law applies?
This question is complicated. If you are working in a transnational team or making statements about foreign players, there may well be more than one country where you could be sued. This is especially the case if your statement is published online and can be downloaded in multiple countries. A defamation lawsuit can usually be brought in the country where:

- the defendant lives (or, in the case of multiple defendants, where at least one of them lives);
- the contested statement was published;
- the damage occurred, or
- the claimant has their/its "centre of interests".

Even if you can identify that you are most likely to face a lawsuit in country A, it is not a given that the court will apply country A's law to the dispute. Each country has its own rules (so-called "conflict of laws" rules) to determine which country's law applies to cross-border disputes.

Therefore it is entirely possible, for example, that a French court decides it is going to apply Swedish law to a dispute.

The good news is that defamation laws do not differ hugely from country to country within Europe, so legal advice that is correct for one country will usually not be wide off the mark for another country.

Can you quote from or link to a source without being liable for the content if it is defamatory?

Suppose you want to publish an interview with someone who makes statements that might be defamatory - would you be legally responsible for those statements? And what about relying on facts from another source - for example, if you write *"the Frankfurter Allgemeine Zeitung has reported that X company sold faulty medical devices..."* would you be liable too if the newspaper got its facts wrong?

The European Court of Human Rights case law is not completely clear on this but you should be in the clear if you observe the following precautions when quoting others or referring to external sources, including by hyperlinking to them:

1. **Only quote, refer to or link to sources that you believe to be credible.** If the source is not a reputable one, or you have specific reasons to doubt that the information is accurate, don't refer to it. However, if the statement's credibility is questionable but it is newsworthy, you can still publish it.

2. **Don't endorse the statement.** Be clear that it's someone else's statement, not yours. Use expressions like "reportedly", "according to" and "has been accused of". Adding footnotes or hyperlinks also helps.

Example

If you have read a seemingly credible NGO report exposing price-fixing by a company, don't write "Company A has a track record of anti-competitive behaviour", but "A report by NGO B found that company B had engaged in anti-competitive behaviour".

Take care not to accidentally treat statements by others as true elsewhere in your text. For example, avoid a heading like *"A history of cheating consumers"* above the paragraph that discusses NGO B's accusations against company A.

3. **Consider whether you need to verify the statement.** Due diligence is expected in responsible journalism and publication. There might be situations where a statement is so damaging that you should verify it before quoting it or linking to it, even if you have no specific reasons upfront to doubt its accuracy or the credibility of the sources.

4. **Always verify information from confidential sources.** If your source is a person who wants to remain anonymous, you need to pay extra attention. If you publish the person's claims and are then sued for defamation, you can probably not count on the source agreeing to help you in your defence, for example by giving a witness statement. Therefore, you should be ready to prove the truthfulness of the source's statements in another way, for example with documentary evidence.

How to arm yourself against a defamation SLAPP

There is no failsafe way to insulate yourself against defamation SLAPPs, but there are steps you can take to meaningfully reduce the risk of a suit, and put yourself in a position to defeat it more quickly and cheaply.

Step 1: Identify all the statements you want to make that could be harmful to reputation

First, identify each statement in your planned publication that could trigger a defamation claim, *i.e.* those that might harm a person's or entity's reputation.

Then identify whether these statements are factual allegations or opinions. This is important because the required proof is different:

- You may be required to prove the truth of factual allegations.
- You are not required to prove the truth of an opinion, but you may be required to show that there is a reasonable factual basis for it. As a rule, the more damaging the opinion is, the stronger the factual basis should be.

Example

It is not always easy in practice to distinguish between facts and opinions: for example, a statement like *"person A's conduct is totally corrupt"* could be understood as a factual allegation that person A broke the law, or as an opinion that person A's conduct is completely immoral (but not necessarily unlawful).

A court will look at the context to decide whether the statement is factual or an opinion, and therefore what level of proof is needed.

When you review your text, it is a good idea to minimise such ambiguity, to prevent a situation where you are required to prove the truth of a statement that you in fact intended as an opinion. In

this example, you may want to write *"I consider person A's conduct totally crooked"* instead, as that is unambiguously a statement of opinion.

Step 2: Prove factual allegations and show a reasonable basis for opinions

The next and key step is to check that you have enough evidence to back up your factual allegations and that you can show a reasonable factual basis for your opinions.

There is no objective standard for what is "enough evidence" or "a reasonable factual basis". You want to make sure you have proof that would be likely to convince an educated person (like a judge) that your factual statements are true and your opinions are not unreasonable.

Here are a few specific pointers:

1. You are entitled to **rely on the contents of official reports from public bodies** without having to undertake independent verification.
2. **Corroborate information from sources:** If you are basing yourself on a human source, corroborate what they are saying: in other words, find additional evidence that removes any reasonable doubt that they are speaking the truth. A single witness may not be believed by the court. And if the source wants to shield their identity and refuses to act as a witness in your trial, you may not have any witness at all.
3. **Don't go beyond your evidence:** Make sure your published statements don't go further than what you can prove.

Example

If villagers you interviewed have reported an increase in cancer since a factory opened nearby, but you have no statistical proof there has been such an increase, don't write *"cancer has spiked in the village since the factory opened",* but rather write something like *"villagers say there appears to have been a spike in cancer since the factory opened"*. If you do have statistical proof of the spike, you should still avoid linking it firmly to the factory unless you have a basis for doing so. So, you could write: *"Epidemiological research shows a sharp increase in cancer cases following the opening of the factory. Further research is needed to determine whether the factory is the cause."*

4. **Be specific about whom you are accusing**: Be careful not to make statements that harm the reputation of third parties that are not involved.

Example

If you are revealing a scandal around the contamination of beef, be clear about which brands are involved (unless all of them are).

Example

When criticising a corporate group, be careful not to conflate entities within the group, as legally speaking entity A may not be responsible for what entity B did.

5. **Quotations and hyperlinks may not need verification:** When you quote or link to third-party statements you do not always need to verify their contents, see the section "*Can you quote from or link to a source without being liable for the content if it is defamatory?*" above.

6. **Less strict standards for statements about politicians, public figures etc.:** As discussed above under *"Who can bring a defamation suit?"*, the limits of acceptable criticism are wider concerning certain influential individuals and entities, such as public bodies, (high-ranking) public officials, politicians and large corporations. This does not mean you don't have to verify your statements about them, but your opinions can be more boldly and confidently stated.

7. **Be aware of other laws:** not every truthful statement can be legally published. For example, there are also laws on privacy and intellectual property.

Step 3: Opportunity to comment

It is a good idea to run your factual allegations by the subject and invite comments before publication. For journalists, this is often a requirement under their codes of ethics. Reasons to provide an opportunity to comment include:

1. It may reveal factual errors that can occur despite rigid research.

Example

A member organisation of CASE was once planning to accuse a fashion brand of sourcing clothes from a problematic garment factory. The fashion brand strongly denied any connection to the factory. In the end, it was revealed that the factory was turning out counterfeit branded clothing.

2. Readers will want to know what the target's response to the allegations is, and presenting that response makes the publication more informative and credible.

3. Obtaining the target's response enables you to contextualise and comment on their position in your publication.

Authors of publications are sometimes concerned that they will lose the element of surprise if they allow the subject(s) of their statement to comment, and that this will enable the subject of the publication to seek a court order blocking publication or to "kill" the story through a PR offensive.

However, the European Convention on Human Rights makes it very difficult to block a story before it is published, and in many cases giving an opportunity to comment helps you prepare for a PR offensive, as the subject of the story will reveal their talking points to you so that you can anticipate them in your final publication.

A few pointers on how to conduct a proper opportunity to comment process:

- You do not need to provide your whole publication but can instead extract any allegations that are harmful to the subject's reputation, and that the subject has not already commented on before.
- Make sure the invitation to comment reaches the right person or department rather than a general or info email address. In some cases, a courier might be a better way to deliver the letter as this ensures the receipt of your letter can't be denied.
- Provide enough time for the comment. This is determined on a case-by-case assessment. It depends on how much time the subject would reasonably need to be able to respond.
- Give proper consideration to any comments received, and make any necessary additions or corrections to your draft.

Step 4: Store your evidence

Make sure to always keep a proper dossier of all the evidence backing up your statements and of your correspondence with the subject of the publication. This is critical because sometimes a lawsuit will only happen much later.

Step 5: Decide on who is identified as the author and publisher

If you want to reduce the risk of individual authors or contributors facing a SLAPP, it can be an idea to leave their names off the publication. Of course, this step should not be taken too lightly, because transparency about the authorship is in principle a good thing.

If there is a range of options, you may also want to think about the best jurisdiction in which to publish as defending a defamation SLAPP is much more expensive in some jurisdictions than others.

Example

The UK is notorious in this respect. It may therefore be a good idea to minimise any unnecessary connections to the UK, that might help a claimant bring a defamation suit there.

Preventing trouble with copyright and trademark law

In this section we look at two areas of intellectual property law that sometimes are abused for SLAPPs: copyright and trademark law.

Copyright law is the area of law that gives rights to the creator of an original work, which could for example be a written text, work of art, musical composition, design, photograph, video, font, or software.

Trademark law protects signs, designs, expressions or other devices that are used to identify products or services. Examples include company or brand logos, catchphrases like “Just Do It”, or distinctive shapes like the Heinz ketchup bottle. Note that a design might in some cases be protected by both copyright and trademark law.

Real violations of copyright and trademark are rife on the internet. There is also a significant problem of unscrupulous or unprofessional companies sending unfounded cease and desist letters or demands for payment to public watchdogs, based on alleged violations of copyright or trademark.

When can you use material that might be copyrighted?
If you want to use material created by someone else for some kind of public expression, you would be permitted to do so in the following circumstances:

1. **If it’s a work that didn’t involve any kind of creative process.** Copyright law only protects works that are the product of some kind of skill, judgment or effort by a human maker.

Example

Footage shot by security cameras could be an example of a recording that is not protected by copyright law, although this might depend on the facts of the case, in particular whether the footage resulted from some kind of creative judgment by the person placing the camera.

A well-known copyright dispute revolved around charming selfies taken by Celebes crested macaques, a type of monkey, using equipment belonging to the British wildlife photographer David J. Slater. Slater argues that he owns the copyright to the images, as the photos were the result of an effort he had made, by visiting and befriending the monkeys, and strategically placing camera equipment. Others, including the Wikimedia Foundation, have claimed that since he is not the maker of the photos, Slater does not hold the copyright. There has not been any court ruling deciding whether Slater has rights to the selfies or not.

2. **If it's a work that no longer enjoys copyright protection.** In EU countries, and most non-EU countries in Europe, copyright protection lasts until 70 years after the death of the author (or 70 years after the death of the last surviving author, if there is more than one). Be aware, however, that a performance or derivative work might still be copyright-protected. For example, Mozart's symphonies are out of copyright, but specific publications or performances of those symphonies may not be.

3. **If the copyright holder has indicated that the work can be used by members of the public.** A popular way (bot not the only way) for copyright holders to do this is to make the work available under one of the standard licences published by the Creative Commons organisation. Most of these licences include limited conditions that you need to comply with if you want to use the work, such as giving credit to the creator, or using it for non-commercial purposes only. It is important to be aware of the specific requirements that apply.

4. **If you obtain individual permission from the copyright holder(s).** Obviously, copyright holders often sell licences to use their work on a commercial basis, but sometimes they are also willing to give a free or reduced price licence to a public interest cause. It can be worth asking.

5. **If a copyright exception applies.** More on that in the next section.

Exceptions to copyright

National copyright laws usually contain various exceptions, allowing the use of copyrighted material without permission from the copyright holder in specified circumstances. EU law (specifically, Directive 2001/29/EC) has created a "menu" of exceptions that Member States can choose to implement. Although this has led to some harmonisation, unfortunately there are still significant differences that make it important to consult your local law or lawyer before relying on an exception, whether you are working inside or outside the EU.

Below is a list of exceptions that are often recognised in national law (also in non-EU European countries), and that are relevant to the work of public watchdogs. Make sure to read the important explanation below before relying on any of these exceptions:

- **Using material as an illustration for teaching or scientific research.** For example, you could incorporate graphs taken from a newspaper article into PowerPoint slides for a university lecture.

- **Using material in connection with the reporting of current events.** If you are making a video about an ongoing disaster at a mine, you could for example use footage of the mine or the disaster to illustrate your story.

- **Using quotations for purposes such as criticism or review.** A quotation normally doesn't need to consist of text, it could also be a sound or visual quotation, like a fragment of a song, video or graphic. The exception allows you to use a quotation if you are reviewing the material you are quoting, or the quotation supports a criticism you are expressing.

- **Using political speeches, extracts of public lectures or similar works.**

- **Use of material for the purpose of caricature, parody or pastiche**. The European Court of Justice has held that a valid parody is a new work that evokes an existing work, while being noticeably different from it, and that expresses humour or mockery. It's not necessary that the humour or mockery is directed at the original work. For example, it is permissible to use a (noticeably altered) Disney character to mock a politician, even if that politician is unconnected to Disney. However, the Court also indicated that a parody shouldn't cause disproportionate harm to the copyright holder. What that means in practice is a bit unclear, but it is something to bear in mind.

Importantly, there are a few requirements that you are likely to have to meet when relying on the above exceptions, other than the caricature/parody/pastiche exception:

- You have to indicate the source and the author of the material, unless it proves impossible.

- The material should really support the point you are trying to make. You shouldn't use it mainly for decorative purposes.

- You shouldn't make more extensive use of the material than is needed to make your point. For example, incorporating a few seconds from a relevant documentary into one of your own videos might be defensible, but uploading the entire documentary to your own website is unlikely to be considered justified.

Copyright pitfalls
Here are a few additional things to watch out for:

- Significantly altering or reworking someone else's work doesn't mean that they no longer have a claim against you. For example, if you artistically edit someone else's photo in Photoshop, you may be creating a new "derivative" work to which you own the copyright, but you would still need the photographer's permission (unless an exception like parody applies).
- If you find material on the internet that is being offered for free use, check that the person/website offering it is credible. It may be that they are giving someone else's intellectual property away.
- Beware of meme generators. Many meme generators allow users to upload images that others can then use to make memes. There is no guarantee that the user who uploaded the image actually had the right to make it available in that way.

- The design of buildings is generally protected by copyright, and in some countries, there are restrictions on how images of buildings can be used.

When can you use trademarks?
There are differences in national laws regarding trademarks, but if you observe the following precautions you should normally be in the clear:

- Don't use the trademark of another, or a sign that is confusingly similar, in connection with any goods or services you offer. For example, if you have a campaign against corporation X, it would be safer to avoid selling t-shirts with a design that includes the logo of corporation X, even if the message is opposed to that company.
- Avoid using the trademark of another, or a sign that is confusingly similar, in connection with fundraising activities, except with permission.
- More generally, avoid any situation where you use the trademark of another, or a sign that is similar to it, in such a way that ordinary people might believe that your activities are actually those of the trademark holder.

Outside the situations discussed above, it is perfectly acceptable to use the logos or other trademarks of a company as a shorthand for that company when discussing it. For example, if you are making a ranking of the 10 best or worst companies in a particular area, you are allowed to include their logos in the ranking, so readers can more instantly recognise whom you are talking about.

Making parodies of trademarks is also generally not a problem, if the purpose is criticism for non-commercial reasons, and there is no risk that the parody will be mistaken for the real trademark.

Preventing trouble with protests

When protests lead to problems, it is more often excessive repression by law enforcement than SLAPPs. However, SLAPPs do occur, especially in response to direct action protests against corporations. This section suggests steps you can take to mitigate that risk.

Step 1: Develop a clear plan for your protest

A detailed and well-designed plan serves several purposes. It ensures alignment between the participants in the protest, reduces the risk of improvisation resulting in unintended consequences; and if you have access to a lawyer, it enables that lawyer to give you more accurate advice.

Examples of things to include in your protest plan include

- What are the specific activities that will happen from start to finish?
- What are developments or escalations that could happen (e.g. arrival of law enforcement) and how will you respond?
- What are the exit strategies?
- What will your slogans/messages be?
- What roles are there and who will fulfil them? Note: it can be a good idea to appoint
    - A person responsible for safety, with a mandate to end the protest if safety cannot be guaranteed any longer
    - Spokespersons to whom all inquiries from the media, law enforcement or the protest target will be directed, to ensure consistent communication
    - Persons who document the protest, to ensure there is an objective record of what happened in case of legal trouble after the event.
- Will the authorities and the target of the protest be notified in advance, and if so, when and how?

Step 2: Assess and mitigate the legal risks

If you are able to, it is always a good idea to get legal advice before a protest, especially a disruptive one.

Examples of good questions to pose to your lawyer in relation to the risk of SLAPPS

- Could the action lead to civil liability, and yes, what compensation might need to be paid?
- Which individuals/organisations could face this consequence, and who is most at risk?
- Are there any defamation risks with the proposed messages/slogans?
- Are there steps that can be taken to eliminate or reduce the risks identified?

If you aren't able to obtain legal advice, and are planning to make statements that are critical of individuals or companies, we recommend reading the section in this Guidebook about preventing trouble with defamation law.

Step 3: Take decisions and prepare for risks

Make an overview of all the risks (legal, security, reputational etc.), the options to mitigate the risks, and decide whether the remaining risk is worth taking when weighed against the expected benefits of the action. If the decision is to go ahead, prepare for the possible consequences: draw up a plan for likely and worst-case scenarios, including who does what, who takes decisions, and how any costs are split. Ensure a lawyer is on standby if needed and possible.

An important decision is who takes public responsibility for the protest, and to what extent individual participants are named. Named persons, especially organisers, are most at risk if the target of the protest decides to file a SLAPP. On the other hand, transparency is an important value, and acting transparently can also help convince a court that the protest was legitimate, and the lawsuit filed in response is not.

Step 4: Prepare participants

Ensure participants in the protest receive a sufficient briefing, covering what they are expected to do, what legal risks they might be running, what kind of support they can expect from the organisers (in particular, what level of legal, humanitarian and financial support will be provided in case of risk materialising). Ensure there is a meaningful opportunity for participants to opt out of the protest without repercussions, if they are not comfortable after the briefing.

Step 5: Delivery of the protest

It is usually a good idea to communicate with the protest target immediately before or at the start of the activity, explaining what you are planning to do, your objectives and demands, the safety precautions taken, and how to reach you to discuss any safety concerns or your demands. These steps can help reduce tensions and prevent a disproportionate response. If you subsequently face a SLAPP, this step may help you convince a court that you acted responsibly and that the lawsuit is excessive. As noted above, it is also a good idea to record the protest, to have evidence to rebut any unfounded allegations. Make sure to have a protocol on gathering and storing these recordings, so you have access to them when you need them.

Preventing trouble with whistleblowing, commercial and official secrets

Introduction

This section focuses on SLAPPs that relate to whistleblowing. Put simply, a whistleblower is a person who reports that a private or public body or individual that they work for is engaging in an unlawful act.

The section focuses on the rules determined by the Directive (EU) 2019/1937 (the EU Whistleblowing Directive) and the European Court of Human Rights' case law.

The European Court of Human Rights' criteria for granting legal protection to whistleblowers slightly differ from those of the European Union Directive. Several key cases clarify the conditions for whistleblower protection, *see box below*.

Scope of the Whistleblowing Directive

The Directive lays down "common ***minimum*** standards" for the protection of whistleblowers within a work context. This means these protections are the minimum that applies in all EU Member States - and in some cases, national law might offer more protection.

There are three basic requirements which must be met to be protected as a whistleblower:

1. Information reported must fall within the material scope of the Directive (step 1 below);
2. The person reporting the information must have been, presently be or about to be an employee of the alleged wrongdoer (step 2 below);
3. The person reporting the information must have reasonable grounds to believe the truth of the information reported and must follow the proper reporting procedures (step 3 below).

Step 1: Material Scope

Information falls within the Whistleblowing Directive if:

- It is about a breach of law in one of the following areas:
  - public procurement;
  - financial services, products and markets, and prevention of money laundering and terrorist financing;
  - product safety and compliance;
  - transport safety;
  - protection of the environment;
  - radiation protection and nuclear safety;
  - food and feed safety, animal health and welfare;
  - public health;
  - consumer protection;
  - protection of privacy and personal data, and security of network and information systems.
- The financial interest of the EU is affected including fraud; or

- It is about a breach of the internal market through circumventing corporate tax laws.

Step 2: Employment Relationship

The person disclosing the information must have been, currently in or about to be in a work-based relationship with the person whose information it relates to. This includes workers, shareholders, persons belonging to the administrative, management or supervisory body, volunteers, trainees and any persons working under the supervision and direction of contractors, subcontractors and suppliers.

This also applies to third persons such as colleagues or relatives and facilitators. A facilitator is a person who assists a reporting person in the reporting process in a work-related context, and whose assistance should be confidential.

Step 3: Reasonable Grounds and Follow Proper Process

The person reporting the information must have reasonable grounds to believe the truth of the information reported and must follow the proper reporting procedures.

Proper Process

The Whistleblowing Directive encourages but does not require individuals to first proceed with an internal report to their employer. If this is not preferred, then they can also directly report the information to the relevant public authorities. The latter approach is known as external reporting.

Note

Public authorities may include a national competition authority or ombudsman. The relevant authorities in a specific country shall be set out in the specific national laws that give effect to the Whistleblowing Directive.

Information may also be disclosed directly to the general public where either: there is an "imminent or manifest danger to the public interest" or if an external report entails a risk of retaliation or low prospects of addressing the breach (e.g. collusion).

General principles of the European Court of Human Rights (ECtHR)

Regarding **public-sector employees,** the Court identified 6 factors that are relevant to decide whether a person is protected under the ECtHR's whistleblowing case-law (*see* Guja v. Moldova case, 2008, app. no. 14277/04).

1) The existence of ***other effective means*** of remedying the situation;
2) The ***public interest*** served by the information disclosed;
3) The ***authenticity*** of the information disclosed;
4) The balance between the ***damage*** caused by the disclosure to the public authority and the interest of the public in having the information revealed;
5) The whistleblower's ***good faith***;
6) The severity of the ***penalty*** imposed to the whistleblower.

The Court confirmed that these factors extend to **private-law employment relationships** *(see* Heinisch v. Germany, 2011, app. no. 28274/08).

The **Halet v. Luxembourg case** (2023, app. no. 21884/18) consolidated the previous case-law and reaffirmed the case-by-case approach depending on the particular circumstances and context of each case.

Protection measures

If you are a whistleblower who meets the requirements of steps 1-3 then you are entitled to confidentiality and protection against retaliation.

Both internal reports made to employers directly and external reports made to public authorities are protected by confidentiality. Your identity should not be disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without your explicit consent. You are entitled to protection of identity for as long as the investigations are ongoing.

As a whistleblower, you are also entitled to not be retaliated against or have attempts of retaliation being made against you e.g. dismissal, demotion, etc.

You are further entitled to protections including not being liable:

- for any kind in respect of the report or public disclosure;
- in respect of the acquisition or access to the information reported or disclosed provided that it did not constitute a self-standing criminal offence; and
- for defamation, breach of copyright, breach of secrecy, breach of data protection rules, disclosure of trade secrets, and/or compensation claims based on private, public or collective labour law, as a result of reports or public disclosures;

Where retaliation measures are taken and/or other protection entitlements are breached then you are entitled to full remedies and compensation for any damages that you suffered.

You are also entitled to the right to an effective remedy and the right to a fair trial, presumption of innocence and rights of defence.

Support Measures

As a whistleblower, you are also entitled to a wide range of support including

- information and advice;
- effective assistance from competent authorities;
- legal aid in criminal and cross-border civil proceedings; and
- May in some countries receive financial assistance and psychological support.
- anonymous reporting depending on the rules set out in a particular country.

Can I disclose information about a private business that is not meant to become public?

Without prejudice to the rules laid out above regarding whistleblowing, there is also a specific legal framework regarding the protection of trade secrets.

The information provided below is based on the EU Directive on the Protection of Trade Secrets of 8 June 2016 against their unlawful acquisition, use and disclosure. The key elements of the texts are simplified below, but always keep in mind that when in doubt, resorting to a lawyer is the safest way to avoid legal trouble.

Trade secrets are **broadly defined**, and so are their use or disclosure.

Basically, an information becomes a trade secret if it meets all three of the following criteria:

1. It is known only to a limited group of persons.
2. It has commercial value because it is secret.
3. It is kept secret - meaning that it has been subject to reasonable steps taken by the person lawfully in control of this information to keep it secret.

Example

Depending on the circumstances, the following elements may be considered as trade secrets:

- early stage inventions, including for instance recipes, algorithms or chemical compounds;
- manufacturing processes and internal business matters such as lists of suppliers or clients, results of marketing studies or prices and dates of launching of new products.

Using or disclosing a trade secret without the consent of its holder may expose you to litigation. However, there are exceptions allowing such use or disclosure, the most important one for the purpose of this guidebook being the exercise of the **right to freedom of expression and information, including the freedom and pluralism of the media**.

This does not prevent altogether the initiation of proceedings, but if you are facing a SLAPP based on the protection of trade secrets, the procedure may be dismissed on the grounds of the protection of freedom of expression and information. This will be more likely to happen if you acted in good faith and did not reveal more than what was necessary to contribute to the public debate.

For more information on the right to freedom of expression, see below: the principles and case-law laid out in the section "Can I disclose information about a public body that is not meant to become public?" are also relevant to the disclosure of information about private businesses.

The other exceptions that may allow you to use or disclose a trade secret are more narrowly defined. You may do so either:

- to reveal misconduct, wrongdoing or illegal activity, provided that you are acting for the purpose of protecting the general public interest;
- in the specific framework of working relationships, you may disclose trade secrets to your representatives, provided that such disclosure is necessary for the legitimate exercise of their representative functions;
- to protect a legitimate interest recognised by Union or national law - but the vagueness of this notion, coupled with the fact that it will be up to the jurisdictions to draw its limits, invites caution.

Can I disclose information about a public body that is not meant to become public?

When considering the disclosure of information about a public body that is not meant to become public, the first step is to **verify whether or not applicable law prohibits it, and if so, what are the sanctions at stake**. States have enacted laws to forbid the disclosure of official secrets, the strictest one being **national defence secrecy** (defined differently among jurisdictions).

However, even if the information falls within a category of protected official secrets (national defence, but also medical secrecy, legal privilege, etc.) prohibiting its disclosure, the ECHR's case law on the right to freedom of expression could, under certain conditions, protect you if you make such a disclosure and could be invoked in the context of a SLAPP.

Generally speaking, members of bodies subjected to certain restrictions, such as military officers, will be more likely to face heavy sanctions for divulging confidential information, whereas journalists and other public watchdogs reporting on issues of general interest are afforded a higher

level of protection, provided that they are acting in good faith and on an accurate factual basis, and provide reliable and precise information in accordance with the ethics of journalism.

The following practical advice is grounded on these general principles:

- Assess whether or not the relevant information may fall under the official secrets category and what do you risk in terms of repression: since these elements may differ greatly from one country to another, the safest way to proceed would be to resort to a lawyer.

- Consider remaining anonymous, especially if you are a member of a particular body subjected to restrictions and obligations of discretion, such as the military.

- Use digital security tools and be particularly cautious on how you transmit sensitive information: store the information on an encrypted hard drive, use Signal instead of other messaging systems, etc.

- If you are a journalist, the steps listed above in the "How to harm yourself against a defamation SLAPP" (p. 7) may also be useful to comply with the abovementioned requirement of acting in good faith and on an accurate factual basis and of providing reliable and precise information in accordance with the ethics of journalism.

Preventing trouble with data protection law

Introduction

There is a growing focus on protecting the rights to privacy and data protection through legislation like the EU General Data Protection Regulation **(GDPR**). Unfortunately, increasingly, wealthy and powerful individuals and corporations are appropriating data protection laws as a means of increasing their tools for silencing journalists and activists.

This section of the guide will first discuss key terminology and when data protection law is applicable. Secondly, it shall provide some pointers on how you can safeguard yourself from falling foul of data protection laws. Data protection law is a complicated area: as with the rest of this Guidebook, what we present here are some simple top lines that might save you trouble if you don't have access to legal advice, which is of course always better.

When does data protection law apply?

Data protection law applies when one processes the personal data of an individual.

Personal data definition: Personal data is any information related to an identified or identifiable living individual. Examples of personal data include a person's name, e-mail address such as firstname.lastname@company.com, photograph and home address.

Processing of personal data:
Basically, any use of personal data is processing. This includes gathering, storing, organising, editing, publishing, deleting and so on. It does not matter what format you use. So for example, data protection equally applies to videos and photographs, social media posts, podcasts, news articles and reports that you may publish. It also generally does not matter who is publishing or using the personal data.

Example

If you are gathering names and signatures for a petition, or inserting a photo of a recognisable individual in one of your publications, you are processing personal data, and you need to comply with your national data protection law and (if applicable in your jurisdiction) the GDPR.

What can you do to ensure that you don't fall foul of data protection law?

As a general rule, you are only allowed to process personal data if you can demonstrate that you have one of these lawful bases to do so:

a. The person consents to the specific use(s) you are making of their personal data;
b. It is necessary for the performance of a contract;

c. It is necessary for compliance with a legal obligation;
d. It is necessary to protect the vital interests of the person or another person;
e. It is necessary for the performance of a task carried out in the public interest and there is a basis in law for the processing; or
f. It is necessary for your legitimate interests or the legitimate interest of a third party except if the interests or fundamental rights and freedoms of the individual outweigh yours.

When determining whether something is 'necessary' a narrow and strict interpretation will be applied. For example, if you were storing the names and signatures of people who signed a petition, you would only be allowed to store their gender if there was a solid explanation why that was needed.

Practical application:
What this means, is that if you want to use personal data in any way, you have to ask yourself whether any of the lawful bases listed in (a.) to (f.) is present. For journalists, NGOs and other public watchdogs, the most relevant lawful bases are consent (a.) and legitimate interests (f.). You might think that (e.) is relevant because it talks about carrying out a task in the public interest; but what is meant here is an individual or organisation that has been given a special role by law, such as a licensed medical practitioner or a water company. This will rarely apply to public watchdogs.

Here is a practical example to illustrate how this works. Imagine you are publishing an article about victims of climate change and you want to add three photographs. Photo 1 shows a family crying outside their half-burnt house and photo 2 shows a person escaping from a flood, badly covered in mud. Photo 3 is the profile photos of the CEOs of the company with the largest carbon footprint globally. Is this all allowed under data protection law?

- The first question you should ask is: do the photos contain personal data? You only need to worry about data protection law if you are using personal data. As discussed above, personal data is information related to an identified or identifiable individual. In this case, photo 1 is likely personal data, as the family members could probably be identified from their faces or their house. Photo 2 might or might not be personal data - it depends whether the person is still identifiable from their appearance or the context, despite being covered in mud. Photo 3 is clearly personal data.

- For those photos that are personal data, the second question is: are you planning to process this personal data? The answer is yes: storing and publishing are forms of processing.

- Then we reach the third question: do you have a lawful basis to process the personal data? Read through the bases above. Only bases a. (consent) and f. (legitimate interests) seem possibly relevant:

    - Check with the photographer whether the persons who are identifiable in the photos of climate victims provided valid consent. Consent is only valid if it is

demonstrable, and sufficiently specific. If the photographer has a signed piece of paper saying "you can use my photo", it would not be good enough, as this is not consent for a specific purpose. On the other hand, if the persons have signed a document that says "I authorise publication of the photographs taken of me today in news media or by NGOs" that would likely be sufficient.

- If there is no valid consent, you can still publish based on legitimate interests if:
  - You have legitimate interests, and
  - Your interests are not outweighed by the privacy rights / interests of the individual(s) concerned.

In this case, you have legitimate interests to process the personal data, because publishing the three photos helps you tell an important story about climate change. But you need to balance this against the impact on the individuals. In the case of the CEO, your legitimate interests will likely outweigh the CEO's privacy interest, as publishing a profile photo of such a famous person does not meaningfully affect their privacy. It is more complicated for the images of climate victims. Might the publication lead to further unwanted attention on them and/or retraumatise them? If children are shown, you have to be extra cautious. There is no clearly correct answer in this case - your job will be to take the decision that seems most reasonable based on all the facts. It can be a good idea to write your thought process down thoroughly. This could help in your defence if you later face a complaint.

Careful

Under many data protection laws including the GDPR, it is prohibited to use or process the personal data that falls in the following special categories unless an exception applies:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership,
- genetic or biometric data,
- health data, and
- sex life or sexual orientation.

Common exceptions to this prohibition include:

- where a person has given their explicit consent;
- where the processing is carried out internally with appropriate safeguards by a not-for-profit body with a political, philosophical, religious or trade union aim and relates solely to current or former members or regular contacts;
- the personal data has clearly and obviously been made public by the person whose data is being processed;
- processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for reasons of substantial public interest.

Countries are also likely to have additional rules and safeguards that relate to processing information relating to a person's criminal convictions or offences.

Please note you may need the consent of the guardian of any child below the age of 16 years if you wish to use their personal data. You will need to consult local law to be sure.

Public figures

Data protection law applies to anyone, also politicians and other public figures who have chosen the limelight. However, the threshold for processing their data (for example, publishing photos or information about them) will be usually lower than for an ordinary person, as you can more easily show a legitimate interest in doing so, and their privacy rights will have less weight – unless the information is unrelated to their public roles and activities. A further consideration for this balancing exercise may be the prior conduct of the person whose data is concerned.

Example

An article about Andrew Julias' drug conviction was reported in the national newspaper. Andrew is a well-known actor who had previously revealed details about his private life in several interviews. He attempted to sue the national newspaper for unlawful use of private information. In deciding whether this case was in the public interest, Andrew's prior conduct was a factor considered by the court. In the court's view, Andrew seeking the limelight curtailed his 'legitimate expectations' to protect his privacy.

Rights of people whose personal data you use

If you are processing someone's personal data, that person (also known as the 'data subject') has a number of rights. The ones you are most likely to encounter are:

- The right of access. The person can ask you to disclose the personal data you hold regarding them, the purpose for which you are processing it, whom you are sharing it with, and how long you will keep it. Such a request is called a "subject access request".

- The right of rectification. The person can ask you to correct mistakes in the personal data you hold.

- The right of erasure. The person can ask you to delete the personal data you hold on them. You don't have to comply, however, if there is still a lawful basis to continue holding the personal data (see the previous section for more details on the lawful bases.)

There have been instances where powerful individuals have used these rights to SLAPP journalists/ NGOs, for example by taking legal action to get access to investigative files compiled in preparation for a publication. Fortunately, as we will discuss in the next section, the GDPR offers some protection against these practices.

The freedom of expression and information exception

The GDPR (specifically, Article 85) requires countries within the EU to implement their privacy laws in a way which balances freedom of expression and the right to privacy. Specifically, EU Member States are required to make exceptions that apply when someone is processing personal data for the purpose of "for journalistic purposes and the purposes of academic, artistic or literary expression". These exceptions don't remove the requirement to have a justification ground for processing of personal data, but they do mean that the rights of data subjects discussed in the previous section (such as the rights of access, rectification and erasure) don't apply.

However, the exact wording of the exceptions is largely left to the country to decide. Some countries (such as Hungary, Romania, Lithuania, and Malta) have implemented laws that do not offer sufficient protection to public watchdogs against SLAPPs based on data protection law.

Example

In some EU member States, only media companies, media services and their employees may use the freedom of expression and information protection under Article 85 when processing data for journalistic purposes. This means that the protection is not awarded (or at least not expressly so) to people outside the media business, such as non-professional journalists, activists and whistleblowers. The failure of the GDPR to require protection for all public watchdogs provides a perfect opportunity for SLAPPs.

An example of this is the case of *Steinmetz and others v Global Witness.* Global Witness is an NGO that reports and campaigns on abuses related to natural resource extraction. After it made allegations that a company called BSG Resources Ltd had obtained a major mining concession through corrupt means, four individuals connected with the company requested access to the personal data that Global Witness held about them, in an apparent attempt to uncover Global Witness' sources. Global Witness refused, basing itself on an exception for "journalism" under the UK Data Protection Act as it stood at that time. The case went to court. In the end, it was decided that although Global Witness is a campaigning NGO that runs investigations, and not a purely journalistic organisation, it could invoke the journalism exception, and didn't have to hand over the data requested.

It is quite possible that courts in other countries would reach the same conclusion, but the UK precedent is not binding on them.

Data Protection Regulator

If someone believes you have breached their data protection rights - for example, by not replying to or complying with a subject access request or request for erasure (see"Rights of people whose personal data you use" above) they may complain about you to a data protection regulator.
The specific steps and process will depend on the law of the country where the complaint is filed. Still, certain steps typically apply, especially if you are based in the EU:

1. Typically the person accusing you of breaching data protection laws will send you a Letter of Demand informing you that they believe you are breaching data protection laws and that they intend to report you to the local data protection authorities.
2. Thereafter, they will lodge a complaint with the local data protection authority.
3. The data protection authority will assess the complaint and get in touch with you and the complainant if they feel they need more information.
4. They will then make a decision.
5. If they think that you have infringed data protection laws then they will often tell you how you can rectify the situation.
6. If they feel that you have not addressed the situation then they may decide to take regulatory action which could include issuing you with a fine.
7. You can appeal a decision taken by a data protection authority. Depending on the circumstances, either a national court or a regional court may be the appropriate way to do this. Contact a lawyer in your country to find out the correct process to follow.

Protecting yourself with insurance

If you are able to get affordable insurance that will cover your legal costs in the event of a SLAPP, it is of course a great way to mitigate the risk. An interesting initiative in this regard is Reporters Shield, a membership programme for print/online media outlets and NGOs that report in the public interest, that offers both financial assistance in the event of lawsuits, and help preventing such lawsuits in the first place, through training, resources, and pre-publication legal checks in high risk circumstances.

What to do if you get SLAPPed

Introduction

It is often very scary or intimidating when you are SLAPPed. You will typically get SLAPPed in four different ways:

1. before you publish, if you have sent the subject of the publication an "opportunity to comment" letter, you might receive a response from lawyers that threatens legal action if you publish what you said you wanted to. They may claim this letter is confidential, although this is likely baseless if you have not yourself agreed to the confidentiality of anything written in the letter.
2. after you publish, receiving a formal letter from the person or their lawyer (Letter of Demand) that says you have infringed their rights and they are going to sue you for damages and/or compensation in a court case and/or report you to a regulatory body that will make you pay a heavy fine. Here too, they may claim this letter is confidential, without any basis..
3. You are issued with a notice or served with a legal claim that the person has opened a court case against you.
4. You are informed by a local regulatory body, for example a national data protection authority, that they have received a complaint that you have violated data protection data laws, and you are asked to respond to the complaint.

Key don'ts:

- Don't panic. Often, threatening letters have deliberately short turnaround times to make you feel more pressurised and/or panicked. Resist the urge to immediately respond and assess your options properly instead.
- Don't sign anything or make any admissions of guilt including apologies both in writing or orally until you have gotten proper advice from a lawyer.
- Don't miss any court or regulatory authority-imposed deadlines. Deadlines set out in a Letter of Demand are often not as important to stick to as these tend to be determined by the party threatening to sue you.

Key do's:

- Contact a lawyer or legal aid centre as soon as possible as SLAPPs are often purposefully complex and confusing.
- Check out CASE's website for additional help or assistance finding a lawyer: https://www.the-case.eu/get-help/
- Find allies and get ready to make a lot of noise about your case, though only after getting proper legal advice, including on the messaging. The purpose of a SLAPP is to silence you, and if the SLAPPer sees the result is the opposite, the case may be over faster.

- Reach out to us! We are here to help you rally support and exert extra public pressure. This effort may include voices of solidarity across Europe and, if applicable, naming and shaming your legal bully.

Court Proceedings

Each court case will be different, however, these steps will likely apply to most situations:

1. You will be served a claim form. This can be intimidating but try to stay calm.
2. You will need to respond to the claim form within the prescribed time. Ideally your lawyer or legal aid centre will be able to advise as to the content of your response and help you respond within the necessary court deadlines.
3. Then each party will be able to present their legal arguments either in written form or orally or both.
4. If the claimant is angry about an ongoing situation - for example, an article that you have published on your website - it may ask the court to issue a temporary injunction against you. This is an order that will be in place until the final judgment of the case, for example instructing you to keep the article offline. Due to the nature of SLAPPs, this can extend for many years.
5. The court will then issue a judgment where they decide who wins the case and whether the other party needs to pay damages or the legal costs of the losing party.
6. Often if the person SLAPPing you loses the case then they are likely to appeal the case as they intend to waste your money and resources.

If you decide not to defend the case then you can settle or admit liability. A settlement is an agreement reached between the parties often used to avoid court proceedings and additional costs. Although this feels frustrating due to the nature of the SLAPP, it may save you money in the long run. Unfortunately, even if you decide you do not want to go to court, and you admit liability, you may still be required to pay the other side's legal costs and some damages. For this reason, you must take time to consider your approach before issuing a retraction or apology as this may still result in you paying an excessive legal bill and/or damages.