REMOTE MOBBING
EXISTS

ByMind

I AM YOU
#PEACE
GLOBAL

Professional preparation of public institutions and non-governmental organizations for systemic counteraction against cyberbullying through the implementation of procedures for the protection of their own staff (risk and image management) and raising the standards of beneficiary service (trauma-sensitive and digitally accessible support), taking into account the specific nature of remote work and international cooperation (PL-BG).

After completing the training, the participants (institution representative) will:

- be familiar with legal responsibilities. Will understand the obligations of institutions as employers in light of the Labor Code (PL/BG) and anti-discrimination regulations (PADA Act in Bulgaria).

- be able to manage crises, to respond to allegations of mobbing within the institution in a way that protects the image of public trust, while maintaining transparency and GDPR compliance.

- use a trauma-informed administration approach, avoiding secondary victimization of beneficiaries reporting violence.

- be able to distinguish between cyberattacks and harassment and know how to secure digital evidence (emails, logs) in a procedural manner.

- understand the mechanisms of cyberbullying against people with disabilities and know how to provide them with support in accordance with accessibility standards (WCAG).

- be able to create a map of local support institutions (PL/BG) and effectively refer beneficiaries (signposting).

- know techniques for counteracting burnout and vicarious stress in "first contact" employees.

Methods:

- Presentation of the legal framework (PL/BG) and definition of cyberbullying.

- Analysis and creation of provisions for internal regulations (e.g. channels for whistleblowers).

- Work on real-life scenarios of image crises and difficult conversations with beneficiaries.

- Instruction on securing digital evidence (creating screenshots with evidentiary value).

- Exercise in building local and international cooperation networks.

- Exchange of experiences between the public sector and NGOs.

Training materials:

- Multimedia presentation containing statistics, legal basis, and procedures.

- Information brochure, a compendium of knowledge for distribution among employees and beneficiaries (digital version).

- Sample "Anti-Mobbing Procedure for Remote Work" and "Irregularity Reporting Form" (for whistleblowers).

- Checklist "Digitally Secure Institution," a checklist covering technical and procedural aspects.

- Technical guide, a short instruction manual on "How to secure digital evidence?"

- Map of Support Institutions. Contact list for PIP, GLI, CPAD, support organizations in Poland and Bulgaria.

Results:

- Institutional strengthening. Implementation or updating of internal procedures (whistleblower protection, anti-mobbing policy) adapted to remote work.

- Professionalization of support. Institution employees will be able to more effectively identify victims of cyberbullying among beneficiaries and provide them with adequate assistance, minimizing the risk of errors.

- Image security: institutions will be prepared to manage media crises related to accusations of mobbing.

- Networking. Local coalitions will be formed between government agencies and NGOs to combat digital exclusion and violence.

- Implementation of the "Green Office." Promotion of digital document circulation and online training as an ecological standard.

- Increased digital competence. Staff will acquire the ability to technically secure evidence of harassment.

Duration: 6 teaching hours

Target group: NGO/authority management, social workers, institutional HR.

ByMind

I AM YOU #PEACE GLOBAL

1. Introduction

Trainer's narrative, explanation of the objectives and expected results of the meeting, e.g. "Welcome to the workshop organized as part of the small-scale partnership project 'Remote mobbing exists! This is a Polish-Bulgarian initiative aimed at developing standards for employee protection in the age of digitalization. Why are we meeting with a group of institutions? Because government agencies, NGOs, and aid organizations have a dual responsibility: to take care of their own staff and to set an example of ethical standards for the private sector."

Establishing rules (Las Vegas confidentiality, openness, respect).

<u>Icebreaker: "Office Mythology"</u>

Task: Participants are to complete the sentence: "In my institution, mobbing is said to be..." (e.g. "...a corporate problem," "...we don't have time for that," "...everyone likes each other here").

Objective: To diagnose mental barriers and denials that exist in the organizational culture of the public/social sector.

2. The law in a nutshell: why do we need to respond?

Poland – employer's obligation (Labor Code):

- o Art. 94 KP: The trainer emphasizes that counteracting mobbing is not a matter of the director's "goodwill," but a statutory obligation.

- o Institutional responsibility. Failure to respond to reports (e.g. of harassment on instant messengers) exposes the institution to lawsuits for damages and compensation, which in the case of budgetary entities constitutes a violation of public finance discipline (payment of compensation due to the employer's fault).

- o Definition of mobbing, reminder of prerequisites: persistence, duration, harassment/intimidation, underestimation of usefulness.

Definition of mobbing:

1. Legal basis:

"Mobbing means actions or behaviors concerning an employee or directed against an employee, consisting of persistent and long-term harassment or intimidation of the employee, causing them to underestimate their professional suitability, causing or aiming to humiliate or ridicule the employee, isolating them or eliminating them from the team of colleagues."

2. Deconstruction of the premises (what does this mean in practice?)

For behavior to be considered mobbing, certain prerequisites must be met. The trainer discusses each of them, giving examples from the digital work environment.

A. Harassment or intimidation is an element of psychological terror. It does not have to be shouting. In remote work, it takes the form of "white gloves." Exerting psychological pressure, intentionally causing distress, threats (overt or covert).

Digital example:

- Sending emails with ambiguous threats ("Think about whether you fit into our team") with a hidden copy to the director.
- "Mute & Humiliate" – muting an employee during a video conference, preventing them from defending themselves, ignoring their presence.

B. Persistence, mobbing is a process, not an incident. The actions are spread out over time and repeated systematically. A one-time argument, even a heated one, is a conflict, not mobbing. Persistence is evidence of the perpetrator's ill will.

Digital example:

- Bombarding an employee with tasks "due yesterday" every day just before the end of the workday.
- Regularly omitting an employee from invitations to team meetings on Teams (not once by mistake, but constantly).

C. Duration. The law does not specify a rigid limit (e.g. 6 months). The Supreme Court indicates that duration is assessed depending on the intensity of the harassment. The more drastic the harassment, the shorter the time needed to consider it mobbing.

In official structures, mobbing often lasts for years because the perpetrator is "irremovable" or protected politically/structurally.

Myth: "It's only been going on for two weeks, so it's not mobbing."
If an employee is publicly humiliated every day for two weeks on video chats, the intensity may meet the criteria for mobbing.

D. An underestimation of professional competence is the goal or effect of the mobber's actions. Destruction of the victim's self-esteem. An employee who was competent begins to doubt their abilities, makes mistakes due to stress, and feels worthless.

ByMind

I AM YOU
#PEACE
GLOBAL

Digital example:

- o The boss orders reports every 15 minutes of work in Excel, suggesting that the employee is "slacking off" at home.

- o Publicly pointing out minor typos on a general communication channel, while ignoring successes.

E. Humiliation, ridicule, isolation. This is the easiest to achieve and the most difficult to prove. It involves cutting off the flow of information (emails, access to files). The employee becomes a "digital ghost." Commenting on the background on the camera, the appearance of the home, ironic remarks about "vacationing in the home office."

Summary for institutions:

- Mobbing and Management.
  Giving work instructions, even firm ones, or enforcing deadlines is not mobbing as long as it does not violate the dignity of the employee. The institution has the right to demand work, but it does not have the right to harass.

- Subjective vs. Objective.
  Whether mobbing has occurred is not determined solely by the victim's subjective feelings ("I feel hurt"), but by an objective assessment of the facts (whether these behaviors objectively violate social norms).

- The role of evidence.
  Remote work leaves a trail (logs, emails). The institution must be aware that this evidence is easy for the employee to secure in the event of a lawsuit.

Bulgaria - protection of dignity and PADA:

- o PADA (Protection Against Discrimination Act): In Bulgaria, harassment is treated as a form of discrimination. The institution must respond immediately if the harassment concerns protected characteristics (age, gender, disability, etc.).

- o Art. 127 of the Labor Code (Protection of Dignity): The employer is obliged to protect the dignity of the employee while performing work (including remote work). Violation of dignity (e.g. public ridicule during a video conference) is grounds for claims.

ByMind

I AM YOU
#PEACE
GLOBAL

Participants must understand that there is no single "anti-bullying law" in Bulgaria. Employee protection is "stitched together" from several legal acts, which forces institutions to respond in a specific way, especially in the context of discrimination.

<u>Protection Against Discrimination Act (PADA)</u>

This is the most powerful legal tool in Bulgaria in the fight against harassment.

In the Bulgarian legal system, harassment is treated as a form of discrimination. The PADA (Art. 5) explicitly states that harassment based on protected characteristics (age, gender, race, disability, etc.) and sexual harassment are considered discrimination.

When does PADA apply? Protection under this law is "activated" when the harasser's behavior affects a protected characteristic of the victim.

Example: If a boss ridicules an employee in a video conference because of his age ("You're too old for this new technology"), this is a matter for the Commission on Discrimination (CPAD).

If a report from an employee/beneficiary contains a discriminatory element, the institution is obliged to immediately initiate an investigation, stop the harassment, and impose disciplinary sanctions.

In Bulgaria, there is a specialized commission (CPAD) to which an employee can file a complaint. The CPAD can conduct investigations and impose administrative sanctions, which is an alternative to going to court.

<u>Article 127 of the Labor Code</u>

This provision fills the gap where there is no discrimination but the behavior is toxic.

Employer's obligation: According to Article 127(2) of the Labor Code, the employer has an absolute obligation to protect the dignity of the employee while performing work.

No definition of "mobbing": The Bulgarian Labor Code does not contain a single, comprehensive definition of "mobbing" as a separate phenomenon, as is the case in the Polish Labor Code (Article 94). Instead, courts interpret mobbing as a violation of the obligation to protect dignity.

Application to remote work: The obligation to protect dignity also applies in full to remote work.

Example of a violation: Systematically sending humiliating emails, isolating an employee from digital communication channels, or publicly criticizing them in a group chat are considered violations of Art. 127 of the Labor Code.

Remote work context (new regulations in Bulgaria)

It is worth mentioning the amendments to the Labor Code (effective from 2024) that strengthened protection in the digital environment:

- Right to disconnect: Bulgaria has introduced regulations according to which a remote employee is not obliged to respond to communication initiated by the employer during their rest time. Violating this right (harassing with phone calls after hours) is a form of cyberbullying.

- Digital monitoring: If an employer uses IT systems to monitor remote work (e.g. reporting, algorithms), they must provide the employee with written information about the scope of the data collected. Covert surveillance is a violation of the law.

Tips for the trainer

Comparison: "In Poland, we have one big 'paragraph on mobbing' in the Labor Code. In Bulgaria, protection is like a puzzle: it consists of anti-discrimination legislation (PADA), dignity protection (LC), and health and safety regulations (psychosocial risks)."

Practice: "That is why it is so important in Bulgaria to determine why someone is being harassed. If the reason is gender/age, we follow the PADA path (very effective). If the reason is 'bad boss', we follow the dignity protection path from the Labor Code."

3. New reality, remote work in institutions

Making participants aware that the digitization of an office or organization cannot mean transferring feudal management habits to the virtual world. Establishing a fine line between necessary supervision and harassment.

A. Moving bureaucracy to the cloud

Public institutions and NGOs are traditionally based on paper and presence ("I see you, so you're working"). The sudden transition to remote or hybrid work in offices often took place without a change in management culture. The result? Communication chaos, which is the perfect breeding ground for mobbing. The lack of clear rules is an opportunity for abuse.

A key problem is that in public trust institutions, employees often feel pressure to be on duty 24/7. In the cloud, this boundary is completely blurred.

B. Limits of control vs. surveillance

The problem of excessive control:

- o Many institutions, distrustful of remote workers, resort to *bossware* tools (software that tracks mouse movements and takes screenshots every few minutes).

- o Interpretation in terms of mobbing. Such surveillance goes beyond monitoring work performance. It can be considered a form of intimidation (harassment) and a violation of the employee's dignity, suggesting their dishonesty out-front. Excessive digital monitoring is identified as a psychosocial risk factor.

Bulgarian best practice:

- o It is worth referring to Bulgarian regulations (the amended Labor Code of 2024), which clearly state that if an employer uses IT systems to monitor remote work (including algorithmic management), they must inform the employee in writing about the type of data collected and the purpose of its processing.

- o Tip for Polish institutions. Transparency is key. If you monitor logs, inform your employees. Hidden monitoring destroys trust and, in the event of a legal dispute, works to the employer's disadvantage.

C. The right to be offline

Legal context (Bulgaria):

- o The trainer points out that in Bulgaria, the "right to disconnect" is explicitly included in the regulations on remote work.

- o Employees are not obliged to respond to communications initiated by their employer during their rest periods (daily and weekly).

Group discussion:

- o *Question to the audience:* "How does this work in your office/foundation? Does a social worker answer calls from clients or their boss at 8 p.m.? Does an official reply to emails on weekends?"

Conclusion: The institution must create procedures (e.g. on-call duty) that relieve individual employees of the burden of being available 24/7. Enforcing non-stop availability is a surefire way to burnout and lawsuits for workplace harassment.

Challenge: Moving bureaucracy to the cloud.

- Limits of control vs. surveillance:

- Discussion of the risks of using tracking software (bossware) in public trust institutions. Excessive control (e.g. screenshots every 5 minutes) may be considered a form of harassment (intimidation).

- *Bulgarian model:* When working remotely, the employer must inform the employee in writing about the scope of data collected (system monitoring).

- **The right to be offline**

  - In Bulgaria, this right is explicitly included in the regulations on remote work – employees do not have to respond to communications outside working hours.

  - *Discussion:* How does this work in Polish government offices/NGOs? Does a social worker answer phone calls in the evening? The trainer points out that forcing 24/7 availability is a prerequisite for mobbing (harassment outside working hours).

Module 1: Institutional Shield – Procedures and Image (45 min)

Module objective: To equip institutions with tools to protect their reputation in crisis situations and to create a functional, safe environment for reporting irregularities (in accordance with the Whistleblower Protection Directive) that effectively protects against the escalation of mobbing.

1. Crisis Management / PR – "When the milk is spilled"

Public institutions and non-governmental organizations rely on social trust as their currency. Mobbing is not only harmful to the employee – it is a betrayal of that trust. In the age of social media, a crisis does not erupt slowly, it erupts suddenly. Today, we will practice how not to add fuel to the fire.

Mini-Case Study: "Crisis in Municipality X"

- Scenario (to be read or displayed): An anonymous post appears on a popular local Facebook group ("Spotted: Municipality X"): *"Mobbing is an everyday occurrence at the Municipality of X. Director Y insults us on Teams, makes us work for free on weekends, and HR remains silent and pretends not to see the problem. We've had enough!"* The post has already been shared 200 times, and the local news portal calls the spokesperson for comment.

- Task for the group: Determine the first three critical steps that the institution must take within the first hour.

Strategy discussion:

1. The principle of transparency and speed:

   - Mistake: The "ostrich" (silence) or "besieged fortress" (attacking the author of the post, threatening legal action for defamation) strategy.

   - Good practice: Immediate release of a preliminary statement (*a* so-called *holding statement*).

   - *Sample message:* "We are concerned about the information that has come to light. Our institution has a zero-tolerance policy for bullying. We are treating this report as a priority and are immediately appointing an independent investigation committee. Until the matter has been clarified, we ask that you refrain from making judgments."

2. Data protection (GDPR) vs. mob pressure:

   - Challenge: The online crowd is demanding the "director's head" immediately.

   - Legal aspect: The institution cannot publicly lynch an employee (even an accused director) before the proceedings are completed. The person must be separated from the process.

   - Message: "Due to labor law and personal data protection regulations, we do not comment on personnel matters before the commission has completed its work. We provide information about the *procedure*, not *names.*"

3. Consistency of communication (Internal = External):

   - Risk: If the Office says "we care about people" in the media, and at an internal meeting the mayor/president shouts, "Who wrote this?! I'll find them and fire them!", credibility is lost. Employees will become a source of leaks to the media, damaging the institution.

   - Good practice: The first message should go to the employees. They need to feel that the institution wants to clarify the matter, not punish the whistleblower.

2. Whistleblowers in practice, building trust

Discussion: How to create a secure reporting channel?

Bad example: A "complaints and suggestions box" hung in the hallway under a surveillance camera or in the office next to the director's desk. It is a sham that no one will use.

Effective solutions:

   - Encrypted online forms: Accessible from outside the office network (e.g. from home), guaranteeing no IP logging.

- o Externalization: A dedicated email address or telephone number operated by an external law firm or auditing company. Employees can be sure that their reports will not be read by an IT colleague who plays soccer with the accused director.
- o Independent ethics officer: A person of public trust within the organization (provided they have a strong position and independence).

Bulgarian context

- Bulgaria has a Commission for Protection against Discrimination (CPAD).
- It is an independent national equality body. If an employee of an institution is afraid to report a case internally (e.g. the head of the institution is the bully), they can file a complaint directly with the CPAD.
- The CPAD has the power to investigate and impose administrative sanctions. This is an important "safety valve" for the system.

The role of trust, breaking down barriers in the budgetary sphere. In Poland and Bulgaria, there is still a mentality that reporting irregularities is "snitching." In small local communities (municipalities, counties), the fear of being "labeled" and retaliation is paralyzing.

The procedure must include a strict ban on retaliatory measures (dismissal, passing over for promotion, transfer to a worse position) against persons reporting in good faith.

Paper will accept anything, but employees are not naive. Even the best anti-mobbing procedure will not work if the organizational culture is based on fear. The implementation of procedures that take into account the specific nature of remote work (where evidence consists of screenshots rather than witnesses in the room) is a sign that the institution understands contemporary threats.

Module 2: Cybersecurity, hard skills (45 min)

Module objective: To equip institution employees with practical skills to distinguish between security incidents (attacks) and harassment (mobbing) and to teach them how to secure evidence that will be useful in investigative or court proceedings.

1. Digital forensics for the layman

Often, victims of cyberbullying come to institutions with emotions but without evidence, or with evidence that is easily refutable. Your task is to teach them (or yourself) how to turn "I feel harassed" into "I have proof of it."

A. Distinction: Hacker or Mobber?

- Hacker/Cybercriminal: Someone who breaks security (e.g., hacks into an email account, steals data). We report them to the police/CERT.

- Bully: Someone who has legal access (e.g. boss, co-worker) but uses it to harass (e.g. sends threats from a work email, deletes files on a shared drive so that the victim misses a deadline). Report to HR/Anti-Bullying Commission/Labor Court.

B. How to take a "legal" screenshot?

- A regular screenshot (e.g. a fragment of a Messenger conversation) can be easily challenged ("It's Photoshop," "It's taken out of context").

- The 3 C rule (What, Time, Whole). For a screenshot to be credible evidence, it must contain:

  1. Content. The offensive message itself.

  2. Sender. Visible first/last name or phone number (not just "Boss," but a specific identifier).

  3. Time. Visible date and time (preferably the computer's system clock in the corner of the screen, not just "5 minutes ago" from the messenger).

Practice: Take a screenshot of the entire desktop (Full Screen), not just a section. This shows the context of your work. Use the PrtScn (Print Screen) key or Win + Shift + S (Snip & Sketch), but keep the taskbar with the clock visible.

C. The "Forward" trap: why don't we forward emails?

The victim receives an offensive email from their boss. They forward it (using the "Forward" option) to their private email account "just in case."

- Why is this a mistake?

  o Using the "Forward" function changes the message headers. The victim becomes the sender (forwarding to themselves), and the date changes to the moment of forwarding. The original metadata (digital envelope) is overwritten or hidden in the content.

  o It is easier to undermine the credibility of such a message in court (the possibility of editing the content before sending).

- Correct operation

    1. Save as a file. Select "Save as" -> .msg (Outlook) or .eml format. This preserves the digital structure of the message.

    2. Print to PDF. Option "Print" -> "Save as PDF." Important: Expand the sender's details so that you can see the full email address, not just the display name.

2. GDPR and surveillance

Remote working has blurred the boundaries. Institutions need to know where employee supervision ends and the violation of their privacy begins, as well as the privacy of the beneficiaries whose data they process at home.

A. Bossware, limits of control

Software for tracking employee activity (e.g. recording mouse movements, taking pictures with a webcam, screenshots every few minutes).

- The perspective of mobbing:

    o Excessive control that does not serve to measure work performance, but only to exert psychological pressure ("I know you weren't at your computer for 3 minutes") is a form of harassment.

    o It signals a lack of trust and an intention to intimidate.

- Legal perspective (Bulgaria/Poland):

    o In Bulgaria, when using IT systems for surveillance (algorithmic management), the employer is required to provide the employee with written information about the scope and purpose of data collection. Hidden monitoring is illegal.

    o In Poland: Monitoring of email/computers is only permitted if it is necessary for the organization of work and the employee has been notified in advance. It must not violate the confidentiality of private correspondence.

B. Home Office Security

A social worker/civil servant works from home. They have sensitive data on their screen (e.g. a benefit application of a domestic violence victim, health data).

- Risks:

    o Household members (children, partner) looking over their shoulder.

    o Leaving the computer unlocked.

    o Using private equipment without security measures (antivirus software).

Good practices (Checklist for institutions):

1. Clean screen rule at home. Locking the computer (Win + L) every time you leave your desk (even to get a cup of tea).

2. Headphones. Conversations about beneficiaries must not be conducted on speakerphone so that neighbors/family cannot hear sensitive data.

3. Privacy screens/filters. If possible, the institution should equip employees with screen filters.

The institution must understand that cybersecurity is not just about "strong passwords," but also about procedures that protect people from harassment (bossware) and data leaks. Knowing how to secure email gives victims of mobbing a sense of agency.

Module 3: Sensitive approach (45 min)

Preparing the institution's employees to assist beneficiaries in crisis in a way that does not exacerbate their trauma, and raising awareness of specific forms of cyberbullying affecting people with disabilities.

1. Trauma, a trauma-sensitive agency.

As employees of an institution, we are often the first "safe haven" for victims. The way we conduct the first conversation will determine whether that person will fight for their rights or retreat into silence. We must move from a "bureaucratic" approach to a "trauma-informed" approach.

A. Language matters avoiding secondary victimization.

Secondary victimization is a situation in which an institution (through inappropriate questions or procedures) causes the victim to relive their suffering.

- Communication analysis (Table for participants):

Instead of saying (Judgmental language):	Say (Supportive language):
"Why are you only reporting this now?" (Suggests that it is too late/suspicious).	*"It's good that you've decided to tell us about this now. We're here to help."*

"Why didn't you just turn off your computer/block your boss?" (Blaming the victim).	*"I understand that you felt helpless in that situation. Bullies can be very manipulative."*
"You must have hard evidence, otherwise we can't do anything." (Putting up barriers).	*"We'll get through this together. I'll explain what documents you'll need and how to secure them."*

B. The mechanism of "freezing" and aggression

- Reaction to stress

    - Freezing. Victims of cyberbullying often do not respond to attacks, do not write back, and do not defend themselves. This is a biological reaction of paralysis, not "silent consent." Officials cannot interpret passivity as acceptance of bullying.

    - Aggression. Sometimes a beneficiary enters the office and shouts.

Tip: "Aggression is rarely directed at you personally. It is often a defense mechanism of a person who has been silenced and humiliated by a bully for months. Your job is to de-escalate, not fight."

2. Disability and cyberbullying

People with disabilities are at the highest risk of cyberbullying because the technology that is supposed to help them can be used as a weapon against them.

A. Specific forms of harassment "Accessibility cyberbullying"

Information exclusion (blind/visually impaired people):

- *Scenario:* A supervisor or co-worker deliberately sends key instructions as scans (images) without a text layer (OCR). A blind person's screen reader only sees "Image 1."

- *Result:* The employee cannot perform the task, therefore is accused of incompetence, and is isolated.

Communication exclusion (deaf/hard of hearing people):

- *Scenario:* Organizing meetings on platforms without automatic captioning options or refusing to turn on the camera (making it impossible to read lips), despite the employee's requests.

- o *Result:* Social isolation and lack of access to information.

Time pressure (people with motor/manual disabilities):

- o *Scenario:* Forcing immediate responses in chat ("Why are you typing so slowly?"), knowing that the employee uses alternative methods of text input.

B. The role of institutions in combating digital exclusion

Accessibility is a right, not a privilege:

In Bulgaria, harassment on the grounds of disability falls directly under the PADA (discrimination) law.

In Poland and in EU projects, the WCAG 2.1 standard applies.

The role of institutions. If a beneficiary with a disability reports mobbing, the official must check whether discrimination is taking place due to a lack of accessibility of work tools.

Module 4: Support system and staff hygiene (45 min)

Changing the approach from "acting alone" to "acting in a network" and equipping institution employees with tools to protect them from burnout resulting from working with people in crisis.

1. You don't have to know everything

Institutional employees often feel pressure to solve every problem a beneficiary has. This mistake leads to burnout. Your role is not to be a lawyer and a therapist in one. Your role is signposting, i.e. being a signpost that unerringly directs people to specialists.

A. Creating a "Help Map"

Task: Together with the trainer, participants build a map of institutions to which victims of mobbing can be referred, depending on their needs (legal, psychological, discrimination).

Purpose of the exercise: To organize participants' knowledge about the competences of individual institutions.

Materials: Flipchart, markers in three colors (e.g. red = law, blue = health, green = NGO).

Exercise procedure (instructions for the trainer):

1. Draw a table on the flipchart with two main columns: POLAND and BULGARIA (for institutions operating across borders or serving migrants).

2. Ask the group: *"A beneficiary comes to you crying and says that his boss is verbally abusing him. Where do you send him?"*

3. Write down the answers, correcting any misconceptions (e.g. that the National Labor Inspectorate can award compensation).

1. Polish pillar

A. National Labor Inspectorate (PIP)

- Role: Control and supervisory body.

- What they can do: Conduct an inspection at the employer's premises, check whether they have implemented anti-mobbing procedures (also for remote workers) and whether they comply with working time standards (e.g. whether they violate the right to rest). They can issue a fine for violations of employee rights.

- What they CANNOT do: PIP inspectors do not rule on whether mobbing has occurred (this is the exclusive competence of the court) nor do they award compensation.

- When should a beneficiary be referred here? When there is organizational chaos in the company, there are no regulations, and mobbing results from management chaos. The PIP protocol can be used as evidence in court.

B. Labor courts

- Role: Judicial authority.

- What they can do: They are the only institution that can legally determine that mobbing has occurred. They can award:

    o Compensation: If the employee terminated the contract due to mobbing.

    o Compensation: For harm suffered and damage to health.

- When to refer the beneficiary here? When the victim has gathered evidence and is ready for a trial.

C. Psychiatrists and Psychologists

- Role: Medical and evidentiary support.

- What they can do: A psychiatrist diagnoses health problems (e.g. depression, adjustment disorders) caused by stress at work. They issue a sick leave certificate (L4), which allows the victim to isolate themselves from the perpetrator.

- Important for institutions: Medical documentation is one of the strongest pieces of evidence in court to confirm the effects of mobbing. Beneficiaries should be encouraged to seek medical help without shame.

2. Bulgarian Pillar

A. General Labor Inspectorate (GLI) – Executive Agency

- Role: Oversees compliance with the Labor Code, including compliance with Art. 127 of the Labor Code, which imposes an obligation on the employer to protect the dignity of the employee.

- Remote work specifics: The GLI also monitors new regulations on remote work, including employers' information obligations in relation to digital monitoring.

B. Commission for Protection Against Discrimination (CPAD)

- Role: Key anti-discrimination body (unique to the Bulgarian system).

- What they can do: They accept complaints from employees if harassment is based on discrimination (e.g. age, gender, disability, race).

- Enforcement powers: The CPAD conducts investigations and can impose direct administrative sanctions on employers. This is often a faster and cheaper route than civil court.

C. Animus Association Foundation

- Role: Non-governmental organization (NGO) specializing in supporting victims of violence.

- What they offer: They operate a 24-hour hotline for victims of violence, including psychological violence in the workplace. They offer psychological and crisis support.

ByMind

I AM YOU
#PEACE
GLOBAL

- When to refer? First and foremost, when the beneficiary is under severe stress, in emotional crisis, and needs immediate conversation ("psychological first aid").

D. Trade unions (CITUB, Podkrepa)

- Role: Collective and individual protection of employees' rights.

- What they offer: Legal support, mediation with employers, representation in disputes.

- Context: In Bulgaria, trade unions (e.g. Confederation of Independent Trade Unions of Bulgaria - CITUB) are a strong partner in resolving internal disputes before going to court.

B. Distribution of Information Brochures

Transforming participants' approach to information materials, from treating them as a "mandatory leaflet" to perceiving them as a functional tool that lightens the workload of officials.

1. Functional analysis of the tool

Discussion of the structure of the Information Brochure, highlighting its four key functions in the daily work of the institution.

2. Channels of communication (brainstorming)

Group task: Participants are asked to map the points of contact between the beneficiary and the institution and to match them with appropriate distribution channels, taking into account the principles of ecology ("Green Erasmus") and digital accessibility.

Recommended discussion topics:

- Digital channel

Use of automation, implementation of a link to the brochure in the email footers of support department employees.
Internal education, placing the material on the intranet as an OHS resource for own staff.

- Hybrid Channel (Phygital):

Replacing mass printing (paperless) with QR code posters in waiting areas (PUP, MOPS, POZ). Quick access to content on the beneficiary's private device, discretion, ecological aspect.

3. Communication modeling.

The instructor discusses three communication strategies accompanying the handing out/sending of the brochure, tailored to the beneficiary's emotional state. The goal is to build a sense of agency in the client.

- Profile A: Beneficiary in emotional crisis (confusion, crying).

    o *Key message:* Empathy and bringing order to chaos. The brochure as a "road map" pointing to safe havens (psychological help).

- Profile B: Beneficiary focused on action (demanding/combative attitude).

    o *Key message:* Professionalism and evidence. The brochure as a procedural instruction (securing evidence, writing complaints) that increases the effectiveness of legal action.

- Profile C: Preventive action (e.g. registering as unemployed).

    o *Key message:* Awareness of rights. The brochure as part of the "employee's essential kit" for entering the remote labor market (protection against working time abuse).

The trainer presents the brochure as a ready-made "first aid tool" that relieves the official of the need to explain the legal basis.

- Distribution strategy (brainstorming):

Placing the PDF file on the websites of public information bulletins of offices, on NGO intranets, in the email footers of social workers. Posters with a QR code leading to the brochure, displayed in the waiting rooms of employment offices, social welfare centers, and health clinics.

2. Occupational health and safety for "helpers"

In order to help others, you must stand on stable ground yourself. Working with victims of mobbing means working with human suffering, fear, and aggression. If you do not set boundaries, you will become the next victims of the system – victims of burnout.

A. Vicarious stress and burnout

- Definition of Vicarious Stress:

It is "the cost of being empathetic." It manifests itself in taking on the victim's emotions, losing sleep over the beneficiaries' issues, and worrying excessively about their fate after working hours.

- Symptoms of Burnout (Red Flags):

Treating the beneficiary as "just another number," "a demanding problem."
Feeling of powerlessness: "Nothing will change anyway, the system is bad."

- Defense mechanism:

Realizing that the official is responsible for the process of providing assistance, not for the outcome (the court's decision or the bully's behavior).

B. Digital Boundaries Techniques

Providing participants with specific communication and technical tools that will allow them to separate their professional and private lives without feeling guilty towards the beneficiary.

1. Diagnosis of the problem "I am available, so I exist?"

Working in a support institution or office carries the risk of blurring boundaries. A beneficiary in crisis does not look at the clock. If you answer the phone at 8 p.m. once, you set a precedent. The beneficiary will consider it the norm. Today, we will learn how to say 'STOP' in a professional manner that does not reject the person but sets the framework for cooperation.

2. The "Iron Curtain" rule

Absolute prohibition: Giving out your private phone number ("only in exceptional cases" is a trap) and inviting beneficiaries to be your friends on Facebook/Instagram.

Risk: A social media profile is a goldmine of information for a demanding client (they can see where you went on vacation while they were "suffering"). This opens the door to hate and harassment.

Solution: Contact only through official channels (office phone, work email, messenger on your work account).

3. Automation, let technology refuse for you

Instruction for the group: "You don't have to feel guilty about not replying after 4 p.m. Let technology do it for you."

Autoresponder template:

"Good morning. Thank you for your message. Please be advised that I work from 7:30 a.m. to 3:30 p.m. and will read your message during that time. In situations of immediate danger to life or health, please do not wait and call the emergency number 112."

Why does it work?

1. It confirms receipt of the message (the customer feels noticed).

2. It defines a time frame (expectation management).

3. It removes responsibility in critical situations (directs to emergency services).

4. Assertiveness workshop, the "Broken Record" technique

Exercise scenario (Pairs): Participants pair up. One person is a demanding beneficiary who calls/writes after hours or demands immediate action ("here and now!"). The other person is

an official who sets boundaries.

Conversation script:

- Step 1: Validate emotions (Empathy).

Do not say: "Please calm down," "I don't have time."

Say: "I can hear that you are upset. I understand that this situation is difficult for you."

- Step 2: Set boundaries (Facts/Law).

Say: "My legal options at this point are to accept the request/write a note."

- Step 3: Time frame (Realism).

Say: "I will take care of this matter tomorrow morning, immediately after the office opens."

Use of the "Well-Rehearsed Script": When the customer presses ("But I want it now!"), the clerk repeats the sequence (calmly, in the same tone): *"I understand that this is urgent, but the system has been up and running since 7:30 a.m. I will take care of your case tomorrow at 8:00 a.m."*

5. End-of-Day Ritual. Stepping out of the role.

Trainer's narration: "In a stationary job, you close the office door and leave. In remote work, the office is in your living room. You have to trick your brain into thinking that work is over."

Discussion examples:

- Physically hiding your equipment: Your work laptop goes into a drawer/bag. If it's lying on the table, your brain is in standby mode ("maybe something came in?").

- Change of clothes: Even at home, it is a good idea to change out of your "work" clothes (shirt) into "home" clothes. This is a signal to your body: "we're resting."

- Border walk: Leave the house for 5 minutes after work and come back – simulating coming home from the office.

Problem: A demanding beneficiary who calls at 8 p.m. or writes to a social worker's private Messenger, expecting immediate intervention ("Because I'm suffering!").

Assertive techniques:

1. Separation of channels: Absolute prohibition on giving private phone numbers and social media profiles to beneficiaries.

2. Automated responses:

Set up an autoresponder after hours: *"Thank you for your message. I will read it during business hours (7:30 a.m. to 3:30 p.m.). In life-threatening situations, please call 911."*

3. The "broken record" technique when talking to a demanding customer:

Customer: "You have to help me now, do something!"

Official: "I understand your frustration (validation). My legal options at this point are to accept your application (boundary). I will take care of it tomorrow morning as soon as the office opens (time frame)."

End-of-day ritual:

Physically and mentally "stepping out of the role" after remote work. E.g. changing from "home" clothes to "work" clothes and back, physically closing the laptop and putting it away in a drawer (so it doesn't "stare" at you in the evening).

Module 5: Implementation and ecology (45 min)

Translating acquired knowledge into concrete actions.

1. Digital ecology in practice

We often think that ecology means waste sorting. In the office, especially a remote or hybrid one, ecology means digitization. Every document that you have not printed but sent via a secure channel saves resources and time.

A. Digitization as a tool for environmental protection

- Paperless office:

Traditional bureaucracy generates tons of paper. Anti-mobbing procedures, regulations, and educational materials (such as our brochure) should only be circulated digitally.

A PDF brochure is not only environmentally friendly, but also easier to update and accessible to people with visual impairments (thanks to screen readers), which is not the case with a piece of paper.

- Reducing your carbon footprint:

Promoting online meetings (instead of traveling to another city for an hour-long meeting) means a real reduction in CO_2 emissions.

Institutions should view remote work not as a "necessary evil," but as a part of a sustainable development strategy (less commuting = cleaner air in the city).

B. "Digital trash":

Digital ecology also means server hygiene. Storing thousands of versions of the same document in the cloud consumes energy. Implementing procedures for archiving and

ByMind

I AM YOU #PEACE GLOBAL

deleting unnecessary emails/files is part of caring for the environment and keeping evidence in order.

2. Implementation plan

The worst training is the kind where we return to our desks and do everything the same way as before. That is why each of you will now make one specific commitment.

Exercise: "Monday declaration"

- Task: Participants receive small pieces of paper (or write in a chat/shared Padlet). They are to write down one action they will take on Monday at their institution.

- Rule: The action must be micro and specific.

Examples of declarations (inspiration for the trainer):

1. *Technical area:* "On Monday, I will send the team instructions on 'How to take a process screenshot with the date and time'."

2. *Procedural Area:* "I will check if our remote work regulations include a provision on the right not to answer phone calls after 4:00 p.m."

3. *Support Area:* "I will print one poster with a QR code for the Brochure and hang it in the MOPS waiting room."

4. *Accessibility Area:* "I will use the WAVE tool to check if our advice website is accessible to blind people."

Summary round: Volunteers read out their declarations. The trainer reinforces the message: "Look, these are small changes, but if each of your institutions implements them, we will create a safety net for hundreds of employees and beneficiaries."

3. Evaluation and closing

Question: "What one thought or emotion do you take away from this workshop?"

Thank everyone for their hard work (the topic of mobbing is a heavy one) and hand out certificates of participation.

Organizational tips for the trainer.

1. If the group is advanced (e.g. HR from large offices), shorten the section on definitions and lengthen the section on crisis management and PR.

2. Remember that there may be people in the room who themselves experience mobbing in their institutions. Observe reactions and ensure discretion.

3. Do not be afraid to admit that change in the public sector takes a long time. Promote the method of evolution (small changes in procedures) rather than revolution.

Attachments:

1. Checklist: "Is my institution resilient to cyberbullying?"

- Do we have a procedure for reporting digital harassment?

- Do employees know how to secure evidence (screenshots)?

- Are the website/materials digitally accessible (WCAG)?

- Do we have a crisis communication plan in case of accusations?

2. Evaluation survey

Appendix 1:

<div align="center">

PRETRAINING TEST

</div>

Please give an honest assessment of your current knowledge. The survey is used solely to determine the starting level of the group and to adjust the focus of the training.
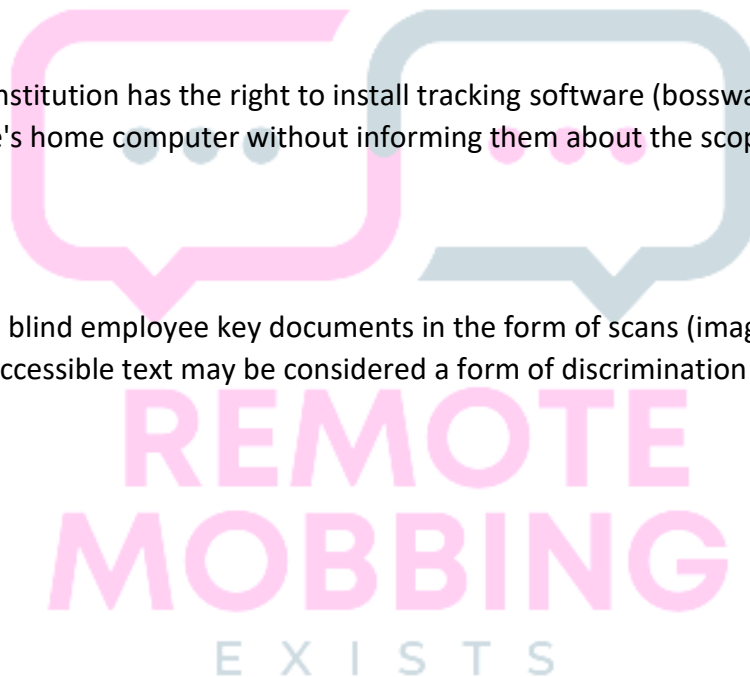
PART A: Self-assessment of competencies

Please assess how confident you feel in a given area at this moment. (Scale: 1 = Definitely do not know/cannot do, 5 = Definitely know/can do)

1. I am familiar with my institution's legal responsibility for cases of mobbing (including remote mobbing) under national law (PL/BG).
   (1) – (2) – (3) – (4) – (5)

2. I know how to secure digital evidence (emails, logs, screenshots) in a manner that is admissible in court.
   (1) – (2) – (3) – (4) – (5)

3. I am able to apply a trauma-informed approach when talking to a beneficiary reporting violence.
   (1) – (2) – (3) – (4) – (5)

4. I know how to manage crisis communication in the event of accusations of mobbing against an institution (media, social media).
   (1) – (2) – (3) – (4) – (5)

5. I am familiar with the map of support institutions in the region (and partner country) to which I can effectively refer a victimized beneficiary.
   (1) – (2) – (3) – (4) – (5)

PART B: Knowledge test

Please select one answer.

1. Using the "Forward" function in your email program is the best way to save an offensive email as evidence.
   TRUE
   FALSE

2. The passivity of a victim of bullying (lack of reaction, silence) often results from a biological "freeze response" mechanism, rather than consent to harassment.
   TRUE
   FALSE

3. In Bulgaria, harassment of an employee on the grounds of age or gender is dealt with by the Commission for Protection against Discrimination (CPAD).
   TRUE
   FALSE

4. A public institution has the right to install tracking software (bossware) on an employee's home computer without informing them about the scope of data collected.
   TRUE
   FALSE

5. Sending a blind employee key documents in the form of scans (images) instead of digitally accessible text may be considered a form of discrimination or harassment.
   TRUE
   FALSE

Appendix 2:

<div align="center">

FINAL SURVEY (POST-TRAINING)

</div>

The purpose of the questionnaire is to assess the increase in knowledge and evaluate the quality of the workshop.

PART A: Self-assessment of competencies

Please assess how confident you feel in a given area NOW. (Scale: 1 = Definitely don't know/can't do, 5 = Definitely know/can do)

1. I am familiar with my institution's legal responsibility for cases of mobbing.
   (1) – (2) – (3) – (4) – (5)

2. I know how to secure digital evidence in a manner that is admissible in court.
   (1) – (2) – (3) – (4) – (5)

3. I can apply a trauma-informed approach when talking to a beneficiary.
   (1) – (2) – (3) – (4) – (5)

4. I know how to manage crisis communication in the event of accusations of mobbing.
   (1) – (2) – (3) – (4) – (5)

5. I am familiar with the map of support institutions to which I can refer beneficiaries.
   (1) – (2) – (3) – (4) – (5)

PART B: Knowledge test (TRUE / FALSE)

Control questions to check acquired knowledge (answer key for the trainer: 1F, 2P, 3P, 4F, 5P).

1. Using the "Forward" function in your email program is the best way to save an offensive email as evidence.
   TRUE
   FALSE

2. The passivity of a victim of mobbing often results from a "freeze response" mechanism.
   TRUE
   FALSE

3. In Bulgaria, harassment based on age or gender is dealt with by the Commission for Protection against Discrimination (CPAD).
   TRUE
   FALSE

4. A public institution has the right to install tracking software (bossware) without informing the employee.

ByMind

I AM YOU #PEACE GLOBAL

TRUE
FALSE

5. Failure to adapt the format of documents to the needs of people with disabilities (e.g. scans for the blind) may constitute a form of cyberbullying/discrimination.
TRUE
FALSE

PART C: Workshop evaluation

(Scale: 1 = Very poor, 5 = Very good)

1. The training content is relevant to my work at the institution/NGO.
(1) – (2) – (3) – (4) – (5)

2. Knowledge about legal and technical aspects was conveyed clearly.
(1) – (2) – (3) – (4) – (5)

3. The materials presented (brochure, checklist, help map) will be useful in practice.
(1) – (2) – (3) – (4) – (5)

4. The way the classes were conducted encouraged activity and the exchange of experiences.
(1) – (2) – (3) – (4) – (5)

PART D: Implementation (Open questions)

1. What **one specific action** (e.g. change of procedure, website audit, team training) do you intend to implement in your institution in the coming week?

2. Which element of the training was the most valuable for you (a "game changer")?

3. What are your ideas for using the project's Information Brochure in your contact with the local community?