3.10. Human rights abuses

A. Despite having clear company policies and processes to ensure respect of human rights, human rights abuses by private security providers may still occur.

GOOD PRACTICES*

Review the risk and impact assessment to ensure all risks and impacts have been properly analysed and all feasible preventive measures are in place (See Challenge 3.1.a.)

- As part of the exercise, assess local capacity to investigate abuses and provide for proper resolution. Risk assessments should "consider the local prosecuting authority and judiciary's capacity to hold accountable those responsible for human rights abuses and for those responsible for violations of international humanitarian law in a manner that respects the rights of the accused." (VPs: 3)

When contracting with a new PSP, require in the Request for Proposals that bidding PSPs are officially registered as per national regulations and provide evidence of business license (See Challenge 3.2.a.)

Ensure the contract with the PSP includes the following requirements and conditions (See Challenge 3.2.c.):

- Refresher trainings on use of force, human rights and international humanitarian law, where relevant, including practical exercises on how to manage security incidents. (See Challenge 3.6.a.)
- A monitoring system. (See Challenge 3.9.a.)
- An incident reporting mechanism. This includes that the PSP reports any incident where personnel "participate in, encourage, or seek to benefit from any national or international crimes including but not limited to war crimes, crimes against humanity, genocide, torture, enforced disappearance, forced or compulsory labour, hostage-taking, sexual or gender-based violence, human trafficking, the trafficking of weapons or drugs, child labour or extrajudicial, summary or arbitrary executions", (ICoC: par. 22) to the client. Contractual obligations towards the client may not be invoked as justifications for such acts.
- A process for investigating reported incidents.
- The right to cancel the contract in case of proven human rights abuses or of humanitarian law violations or to remove personnel involved in credible allegations of human rights abuses or humanitarian law violations.

Establish an early alert system and engage in pro-active monitoring

- Develop a company policy and internal process to deal with both potential and actual human rights abuses and ensure all company staff is familiar with these.
  - Provide human rights training to employees, including on how to identify signs of potential human rights abuses.
  - Designate focal points within the company (e.g. a security manager, a community relations officer) that will receive oral or written reports of potential and actual human rights abuses. Ensure their contact details are distributed to all relevant stakeholders.
  - Require systematic reporting of all alleged and confirmed human rights abuses.
- Monitor causes and triggers of conflict on a regular basis, especially in volatile environments and establish a concrete action plan to prevent and mitigate risks of escalation.
- Monitor PSPs through a variety of means: radio networks, CCTV visual monitoring (including installing cameras in vehicles) and unannounced physical site inspections.
- Support the oversight of the private security sector by local authorities and community groups. (OECD: 215)
  - Develop a network with relevant stakeholders, ensuring the different groups in local communities are adequately represented (in particular the most vulnerable groups), and provide them with some guidance and capacity support – directly or indirectly – on what to do whenever there is a risk of a human rights abuse.
- Encourage dialogue and "local cooperative agreements between security providers and communities that outline the roles and practices of the different actors in maintaining local security, law and order". (OECD: 215)

Establish an operational-level grievance mechanism that allows individuals to report an abuse anonymously

- Establish at least one of the following mechanisms (MIGA: III-16):
  - A report abuse hotline, either via phone or SMS.
  - A secure e-mail address that is solely accessible by a trusted monitor.
  - Tip boxes, with clear instructions posted above them, located in areas where individuals have "unobserved access to the boxes and can drop in anonymous notes, tips or other information".
- Consult with local communities during the design of the grievance mechanism to ensure it is culturally appropriate and that they are able to access it effectively.
- Ensure procedures are "fair, accessible and offer effective remedies, including recommendations for the prevention of recurrence." (ICoC: par. 67)
- Ensure the grievance mechanism "does not have to wait until an issue amounts to an alleged human rights abuse or a breach of other standards before it can address it." (UNIG: 68)
- Make the grievance mechanism "known to, and trusted by, those stakeholders for whom it is intended". (UNIG: 65) This may be done by organising meetings with local communities, or by publishing details of the grievance mechanism in prominent places as well as on a publically accessible website.
- Ensure that those "who report wrongdoings in good faith are provided protection against any retaliation for making such reports, such as shielding them from unwarranted or otherwise inappropriate disciplinary measures, and that matters raised are examined and acted upon without undue delay." (ICoC: par. 67)

- Keep records of all known alleged human rights abuses by private security, whether or not a grievance is raised.

Conduct investigation into credible allegations and, where appropriate, report abuses to the relevant authorities

- "Investigate allegations promptly, impartially and with due consideration to confidentiality". (ICoC: par. 67)
- Ensure that investigation teams are gender-sensitive and, if possible, are familiar with community and/or ethnic or tribal dynamics, and language.
- "Collect necessary information from internal and external sources to determine if allegation is credible and warrants an official investigation". (IGTs: 56)
  - Request an incident report from the PSP as established in the contract. Reports by the PSP should cover "any incident involving its personnel that involves the use of any weapon, which includes the firing of weapons under any circumstance (except authorised training), any escalation of force, damage to equipment or injury to persons, attacks, criminal acts, traffic accidents, (and) incidents involving other security forces" (ICoC: par. 63); and they should provide information on:
    - "Time and location of the incident;
    - Identity and nationality of any persons involved including their addresses and other contact details;
    - Injuries/damage sustained and how established;
    - Circumstances leading up and immediately subsequent to the incident; and
    - Any measures taken by the (PSP) in response to it", including any interaction with victims or witnesses. (ICoC: par. 63)
  - Quickly establish the basic facts (BP: 15):
    - What happened,
    - Who was involved,
    - Whether the business caused the event either directly or through its contractors and security providers, and
    - What is the actual or potential severity of the event.
- Keep records of all findings from the investigation.
- If an incident appears credible and serious, notify senior management and the relevant regional security advisor. (BP: 15)
- Based on the available information, "decide if (the) investigation should be conducted internally or by a responsible third party". (IGTs: 56) "Where an incident triggers significant concern from external stakeholders, consider commissioning an external investigation." (BP: 15)
- Where appropriate, report the abuse to "one or more of the following: the competent authorities in the country where the acts took place, the country of nationality of the victim, or the country of nationality of the perpetrator". (ICoC: par. 37)
- If the host government is to lead the investigation formally express the company's willingness to assist and cooperate. (BP: 15) Do "not participate in or tolerate from their personnel, the impeding of witnesses, testimony or investigations". (ICoC: 67)

"Pursue appropriate disciplinary or remedial actions" (IGTs: 56)

- "Prevent further escalation of the disruptive event". (PSC.1: 25)
- Where force was used, ensure that medical attention is provided to injured parties. (VPs: 6)
- "Determine proper course of disciplinary or remedial action based on outcomes of investigation". (IGTs: 56)
- Provide for or cooperate in the remediation of adverse impacts the company has caused or contributed to through legitimate processes. (GPs: 24)
- Take measures to "terminate business relationships with providers who have been found to have violated international humanitarian law or to have committed human rights abuses". (IGTs: 56)
- If the investigation is led by law enforcement authorities, "actively monitor status of investigations and press for proper resolution". (VP: 6)
- Cooperate as much as possible with investigations conducted by other legitimate actors (e.g. by ombudsman institutions, national human rights institutions, regional human rights commissions or multi-stakeholder initiatives).

Track effectiveness of response on the basis of "appropriate qualitative and quantitative indicators" and drawing on "feedback from both internal and external sources, including affected stakeholders" (GPs: 22)

Conduct lessons learned exercise

- Wherever a significant human rights impact has occurred, initiate a process to identify how and why it occurred. This is important to prevent or mitigate its continuation or recurrence. "If the evidence is sufficiently clear, linking this kind of analysis to staff incentives and disincentives, whether financial compensation, promotion or other rewards, can play an important role in helping embed respect for human rights into the practice of the (company)." (UNIG: 54)
- "Make appropriate changes to contracts, deployment, conduct or (work) with new private security providers, as appropriate, in order to prevent a recurrence." (IGTs: 56)
- "Provide supplementary training to private security providers, where applicable." (IGTs: 56)
- If appropriate, consider using the incident for practical exercises in future trainings.
- Consider whether and how to engage external stakeholders, (e.g. affected communities, civil society organisations) in the after-incident assessment and remediation activities.

Communicate how the company addresses its human rights impacts to all relevant stakeholders, particularly in the event of an incident that generates significant external stakeholder concern and publicity

- Ensure communications are accessible to its intended audiences (e.g. use billboards, posters, website). (GPs: 23)
- "Provide information that is sufficient to evaluate the adequacy of (the company's) response to the particular human rights impact involved". (GPs: 23)
- Consider sharing the 'lessons learned' with other companies working in the area.

GO BACK TO LIST OF CHALLENGES

* These good practices are not meant to be prescriptive. It is up to the user to evaluate whether they could be feasible, useful and appropriate to the local context in a specific situation on the ground.

1. In this chapter the term "Companies" refers to corporate clients who engage the services of a private security provider. Private security providers are always referred to as "PSPs" or, in some quotes, as "PSCs" (private security companies).
2. http://www.securityhumanrightshub.org/content/risk-impact-assessment
3. See "Business and International Humanitarian Law: an introduction to the rights and obligations of business enterprises under international humanitarian law", ICRC, 2006.
4. By Oliver Cushing, Head of Business Development, Tsamota Natural Resources, and Mark Camilleri, General Counsel, Tsamota Ltd.
5. International Stability Operations Association (ISOA) Code of Conduct.
6. Ibid.
7. Ibid.
8. A full list of member companies can be found at: www.icoca.ch
9. South Africa's Private Security Industry Regulatory Authority
10. ASIS International's Management System for Quality of Private Security Company Operations includes PSC 1- 4 standards. PSC 1 will soon be an ISO standard.
11. UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials, par. 5.
12. Socio-Economic Assessment Toolbox (SEAT), version 3 (AngloAmerican, 2012), p. 134.
13. Good Practice Guide: Indigenous Peoples and Mining (ICMM, 2010), p. 47.
14. Ibid.
15. Ibid.
16. Ibid., p. 51.
17. Socio-Economic Assessment Toolbox (SEAT), version 3 (AngloAmerican, 2012), p. 133.
18. Good Practice Guide: Indigenous Peoples and Mining (ICMM, 2010), p. 47.
19. Ibid., p.18.
20. Ibid., p.30.
21. Ibid., p.32.
22. Socio-Economic Assessment Toolbox (SEAT), version 3 (AngloAmerican, 2012), p. 138.
23. OECD Guidelines for Multinational Enterprises, 2011: p.32.
24. From Red to Green Flags: The corporate responsibility to respect human rights in high-risk countries (IHRB, 2011), p.4.
25. Ibid.
26. Ibid.
27. Ibid.