Project new work

In the project “New Work”, The Beacon has tested technology to make the office safer, healthier, and more productive. This technology works best when the preconditions are also in place. Therefore we relied on different experts who shared their best practices regarding privacy, security, and communication. The manual can be used by building owners and managers - public or private - who want to use equipment such as cameras and sensors to control access or crowding.

THE BEACON

www.thebeacon.eu
contact@thebeacon.eu

Sint-Pietersvliet 7,
2000 Antwerp

The 10 communication commandments for tech lovers

Niel Van Herck
Strategic and content director

SUPERMACHINE is a creative agency. They make things people want and they make people want things. Through humanizing strategy, community building and creative campaigning SUPERMACHINE brings innovation closer to the right audience.

01

Think before you talk

Whatever the message will be, creativity always works better with a hint of strategy. So before communicating to the world, you need to ask yourself some questions. What does my target audience need? How can I reach them? When should I speak and when should I be silent? What channels to use? What tone-of-voice? What's the communication goal? Are there internal (staff, values, ...) and external (competition, trends, ...) factors involved? In order to be consistent, efficient and effective, you need a plan.

PRACTICAL

Build a content calendar, analyze your own channels, SWOT analysis is your friend, do some trend watching and read the other nine communication commandments.

TOOLS

Google Trends, Google Analytics, Primer

02

Listen before you speak

Communication is not only about hearing the other person. It's about understanding them and vice versa. Don't forget we all grow up with our own set of values, knowledge and personal experiences. Good communication requires you to use those when effective but to shake them off when they are an obstacle to your target audience.

PRACTICAL

Ask questions, put up surveys, talk to people, invite the target group for events and workshops, use a social listening tool, ...

TOOLS

Forms, Hootsuite, Mailchimp, Twitter search

03

Know who you're talking to

Henry Ford once said: "if I had asked people what they wanted, they would have said faster horses." Get to know your target audience, and be sure to go deep. Are you targetting the right audience? What do they need and what triggers them? How do they feel when using your product? What are the barriers and struggles they have? Which problem can you solve? What channels do they use? What's their behaviour and can we change that? And of course, how do they think about your brand/product? Translate those answers into one key insight. F.e. Nike saw their runners often feel lonely, so they created Nike+, a runner's club.

PRACTICAL

Use data, which can be found in analytics (web, social) and via surveys. Analyse conversion funnels, ask questions and create a persona. That's a fictional person to represent the different user types that might use your service, product, site, or brand in a similar way. Map out the channels they use and the channels you have.

TOOLS

Social Analytics, personae templates, Keyword research, user reviews, the coffee machine

04

One message to rule them all

Buy this, do that, change all, read me, click here. A common communication mistake is telling too much with one action. The golden rule is one message per communication outing. So kill your darlings, and strip down the message to one key takeaway. What is the ultimate goal of your communication? What do you expect from your audience? What's the noise in your communication?

PRACTICAL

Start at the end. What's the end result (KPI's) you're trying to achieve and with whom? Once you know that, choose your channels, create the message and adapt.

TOOLS

SimpleKPI, Google Analytics

05

Make it human

The strongest brands and communicators are those using empathy, in both ways. As humans, we like to connect to humans. As a brand, you should strive to be as human as possible. The way you speak is a big one, the way you listen even bigger. Try to put some emotion in your message and connect to the true desires of your target audience. Don't sell a mattress, sell a good night's sleep. By the way, some imagination and creativity never did anyone harm. Even Ikea succeeded in creating empathy for a lamp: check out their lamp commercial of 2002.

PRACTICAL

Use the 12 archetypes by Jung to define what type of brand you are and adjust your tone-of-voice. It's not obligated to be funny, but try to show your human side. Add personal anecdotes when relevant. Write the rules down, so everybody inside the company speaks the same language.

TOOLS

Jung's archetypes, Coostco tone-of-voice generator, Grammarly

06

Make it grandma proof

A common communication pitfall is foreknowledge. You know your product, brand and message by hard, but your target audience doesn't. It's a trap! These are not the words you're looking for. So don't overcomplicate your message and be sure to test out if your target audience gets what you mean. If grandma knows what you're talking about, you're good to go.

PRACTICAL

Avoid an overdose of jargon, don't use passive phrases, use active verbs and powerful adjectives, use examples and cases, explain complex definitions and don't assume your audience knows every person you know.

TOOLS

Hemingway, Google Forms, A/B-testing, your grandma

07

Show don't tell

It's a cliché but an image really says more than a thousand words. Communication containing visual support has 93% more engagement than plain text. Whether you choose a video, still images or infographics depends on the budget, your target audience and the channels you use. But one thing's for sure; don't go full-on stock photography. At least not the classic ones. Stock photography often adds a feeling of fakeness to the message. Do show your research, it will help your credibility.

PRACTICAL

We like to see faces but if you show people, make sure they are appealing to your target audience. Never use low-quality images, people love infographics and content made by your audience (user-generated content) is a great way to connect. But most important of all, stick to your brand guide and corporate identity.

TOOLS

Canva.com, Pexels.com, Unsplash.com, VSCO, Instagram

08

Don't point the finger, unless it's a thumbs up

People like to be guided by peers, companies and brands, but we don't like to be told what to do. Especially now, with the Covid rules dominating our lives. At all time, avoid a condescending tone. Your customer is the hero, you are the weapons he/she can use to overcome obstacles. Try to be an uplifting brand, a true added value to the lives of your target groups. By the way, do ask yourself who needs to be talking. Is it you? Your team? The brand? Maybe a (business) influencer or one of your customers?

PRACTICAL

Use positive messages, take fear and obstacles away, keep your audience in the lead and don't give the impression that you're better/smarter than your audience. You're a guide, open for interaction.

TOOLS

Hashtags on social to find influencers, Upfluencen, intrawebs

09

Context is all

Read the room. Your communication always has a setting. Whether it is the environment, the social activity, the goals of the group, the people involved, social dynamics etc. You'll speak differently to a colleague at work than in a bar, and you'll change your tone-of-voice when speaking to your boss. Find the balance between formal and informal, and don't forget the hallway communication. What is your team communicating?

PRACTICAL

Consider the physical context. Speaking at an office or in public? Adapt your channels to the message and vice versa. Social dynamics are important, you'll communicate differently to customers than to suppliers. Same thing for timing. There's a difference between communicating in a crisis or communicating when all goes fine.

TOOLS

Analytics, the coffee machine

10

But what should I do?

Unfortunately, we (still) aren't a nation of mind-readers. So you have to be specific on what the expectations are. What do you want the target audience to do, what's the next step? Do they need to subscribe? Maybe they need to click a button? Or is it a social share you're after? Just ask, f.e. when tweeting and literally asking for a retweet, you have 51% more chance of being retweeted. Be clear and brief in your call to action.

PRACTICAL

You should end your message with a powerful, yet uber clear call to action. Use command verbs explaining the action: not "click here for the brochure" but "download our brochure". Next to that, give your audience a reason to interact. Download and learn, subscribe and be the first, ...

TOOLS

Calls-to-action by Hubspot, Optimizely, Hemingway, ProWritingAid

The 10 commandments for privacy & intelligent camera systems

Mathieu Le Boudec
Senior Associate

Anneleen Vander Elstraeten
Managing Partner

Four & Five is a future-oriented business law firm with a laser focus on corporate and commercial law, M&A, IT law, technology, GDPR and real estate. We combine deep legal knowhow with a fresh and focused mindset.

We regularly perform GDPR assessments, draft data processing agreements, draw up privacy policies, and in general, guide our clients towards GDPR-compliancy.

FOUR & FIVE
SMART LEGAL SOLUTIONS

01

Take into account the very broad scope of privacy legislation

The General Data Protection Regulation (better known as the famous "GDPR") applies as soon as you process personal data:

- Personal data you say? The term includes all data relating to an identified or identifiable person. Email addresses, camera images, age, sex, location, ...
- The term "processing" encompasses almost all actions that can be performed on personal data, such as recording, structuring, modifying, retrieving, consulting, using, disclosing, erasing, etc. Nearly everything, right?

In certain cases, specific regulations may apply in addition to GDPR, e.g. the Camera Act regarding the installation and use of surveillance cameras or specific rules concerning camera surveillance on the work floor. Such specific regulations are not in scope of these commandments.

02

Make clear agreements with the other parties involved

The GDPR distinguishes between two main categories:

- The **controller** determines the purposes and means of processing
- The **processor** can be compared to a contractor that processes personal data on behalf of the controller and not for its own purposes.

As a controller, you may only rely on processors that offer sufficient guarantees in terms of compliance with privacy legislation and an agreement is obliged. Pick right!

Most obligations under privacy legislation are imposed on the controller. Be well aware of what role you are taking prior to installing an intelligent camera system. After all, in many circumstances, the customer acquiring and/or installing a camera system may - without realizing it - be qualified as (co-)controller.

03

Only collect and process personal data if necessary

A core principle of the GDPR is the data minimization principle which means that you may only process those personal data that are really necessary to achieve your intended, predefined and lawful goals.

This means you may only install a system based on cameras if the intended purpose cannot reasonably be achieved in another, less privacy-intrusive, way.

04

Never keep personal data longer than necessary

It is important never to keep personal data longer than necessary to achieve the intended purposes. Once the personal data are no longer required for the achievement of the intended purposes, the personal data should be anonymized (which is rather difficult in case of camera images) or removed. So don't stock up on data.

05

Make sure that there is a legal basis for all your processing activities

A controller is only allowed to process personal data if such processing is based on one of the legal grounds for processing. It is an often-heard misconception that you can only process personal data with the consent of the persons concerned. That's simply not true.

In fact, the consent of the persons concerned will only in exceptional circumstances be a suitable ground for processing by means of cameras. After all, in order to be able to rely on consent, it is required that all persons who are filmed have given their prior consent. Employers should even avoid relying on consent for the processing of personal data of their employees. According to the privacy authorities, it is often impossible to obtain valid employee consent due to the imbalance of power between employers and employees.

06

Be transparent about how you handle personal data

Transparency is a key obligation under the GDPR. Draw up a privacy policy that contains at least all the information required by law, including what data you collect, why you do this, how long you will retain that data, where people can go with questions, what rights the persons concerned have, etc. Also make sure that the persons concerned can effectively consult this privacy policy, e.g. by making the policy (or at least a summary with a link to the full policy) available at the entrance of the building in which the camera system is installed.

07

Respect the rights of the persons concerned

Each person whose data is being processed has a number of rights, including the right to be informed about the processing, to obtain a copy of his/her personal data, to be able to rectify any errors, to request erasure of the personal data, etc. A controller must make sure that it is able to respond to such requests.

08

Think about privacy right from the start

Especially in the context of innovative projects, attention must be paid to privacy as from the design phase and throughout the development process of new products, processes or services that involve the processing of personal data.

When processing activities involves a high risk for the privacy of the data subjects, it is mandatory to carry out a prior risk analysis (a so-called Data Protection Impact Assessment or DPIA). The Belgian Data Protection Authority has drawn up a list of activities for which the performance of a DPIA is always mandatory, such as a large-scale processing of data generated by devices with sensors that send data over the Internet or via another medium.

As a result, it will often be required to carry out a DPIA prior to implementing an intelligent camera system.

09

Guarantee the security of the personal data

You must take appropriate technical and organizational measures to guarantee the security of the personal data you process. The concrete measures may vary according to the risks and scope of the processing, the cost and technical feasibility.

10

Be able to prove your GDPR-compliance

According to the accountability principle, controllers must be able to demonstrate their compliance with the GDPR. This means in practice that several decisions and practices must be documented, including decisions regarding the above mentioned best practices (e.g. the agreements with the other parties involved, the purposes for which the personal data are collected, the applicable retention terms, any data breaches that have occurred, etc.)

The 10 commandments of IoT security

Cédric Bassem
Manager - IoT Security

NVISO is a cyber security consulting firm with offices in Belgium (Brussels) and Germany (Frankfurt, Munich). NVISO is exclusively focused on cyber security services, and has extensive expertise in security-critical industries such as financial services, government & defence and the technology sector. NVISO's people are recognized experts and actively present at major security conferences and teach at Universities, High schools and the SANS Institute: expertise and knowledge transfer is part of our DNA.

This unique "skill blend" allows them to analyse and respond to complex client challenges and help those companies prevent, detect and respond to security challenges with a positive business outcome.

Built on values of Pride, Caring for our people, Breaking Barriers, and fostering a no-BS approach, our mission is to be an innovative, trusted and respected security partner for our clients.

nviso

Camera- and sensor-based systems have been successfully implemented to monitor and control crowdedness, or to ensure social distance between people. But there's a but! These systems are more than often connected to the internet, which poses challenges in terms of security. The information recorded is often of a sensitive nature – see Privacy – and as a building owner or manager, you should take the necessary precautions to preserve the security of the Internet of Things devices (camera or sensor), their physical properties and their connection to local or cloud servers and storage systems.

No worries, you can make a good start by implementing these ten commandments!

01 The ground rule for all IT applications, and especially for security sensitive IoT devices, is to use a unique, personal and strong password per device. A strong password has many characters and a high complexity.

02 With many IoT devices, managing all of these passwords can become a challenge. Password managers allow you to securely store all of your complex passwords and allow you to manage who has access to the credentials.

03 Trust is good, but control is better. Ensure only authorized employees or staff can have access to the devices, their management applications and the data generated by these devices.

04 Operational critical data such as configurations and sensor data, needs to be backed up regularly and stored in a secure location, whether on premise or in the cloud.

05 A common mistake is to connect IoT devices to your office network. To avoid that compromise of an IoT device propagates throughout your office network, try to use dedicated IoT networks that are properly segregated from your office network.

06 Don't forget about updates. Favour devices that update themselves over devices that require manual actions. When devices do require manual intervention for updates, make sure to update them on regular intervals or when critical security updates are available.

07 In case of wired systems, be sure to hide the wires so they can't be tampered with. You don't want strangers to either cut or directly connect to your wiring.

08 Don't expose devices directly to the internet. Make use of a VPN, or use the cloud solution of your vendor to allow remote interaction with your devices.

09 Logs are your friend if it goes haywire. Aggregate logs to a central logging server and configure alerting, if this is supported by the device.

10 And lastly, if one of your devices or systems is compromised, make sure to isolate it to avoid further contamination. Unplugging the internet cable is always a safe thing to do and asking for help is even better!