

2026/April - www.fgfc.lu

Impulse für eine zukunftsorientierte Verwaltung

Die FGFC begleitet das Gemeindepersonal in der digitalen Arbeitswelt

Die FGFC hat angekündigt, sich verstärkt mit den Herausforderungen und Chancen der digitalen Arbeitswelt auseinanderzusetzen.

In diesem Kontext stellt sie dem Gemeindepersonal praxisnahe « **Best Practices** » zur Verfügung, um den Arbeitsalltag sicher und effizient zu gestalten.

Der vorliegende erste Beitrag widmet sich der Handhabung von **Cyberüberwachung am Arbeitsplatz** – einem Thema, das angesichts der zunehmenden Digitalisierung von zentraler Bedeutung ist.

Ziel ist es, Mitarbeitende für Risiken zu sensibilisieren und gleichzeitig konkrete, umsetzbare Handlungsempfehlungen zu geben.

Mit dieser Initiative startet die FGFC eine **Serie von Artikeln**, die darauf abzielt, das Gemeindepersonal nicht nur theoretisch, sondern vor allem **pragmatisch und alltagsnah** zu informieren und zu unterstützen.

Parallel dazu wird die **Académie publique** in Zusammenarbeit mit der **FGFC** und dem **Digital Learning Hub** gezielte **Weiterbildungsseminare** zu digitalen Themen anbieten. Diese ergänzen die schriftlichen Inhalte durch praxisorientierte Schulungen und ermöglichen es den Mitarbeitenden, ihre Kompetenzen kontinuierlich auszubauen.

Die FGFC zeigt damit, dass sie **am Puls der Zeit** agiert und ihre Mission weiterentwickelt: Neben der klassischen Vertretung und Verteidigung der Rechte des Personals legt sie einen besonderen Fokus auf **Prävention, Information und Weiterbildung**. Damit leistet sie einen aktiven Beitrag dazu, das Gemeindepersonal bestmöglich auf die Anforderungen der digitalen Zukunft vorzubereiten.

Cybersüberwachung

Dieser Beitrag eröffnet die Artikelserie zur digitalen Arbeitswelt und behandelt das Thema **Cyberüberwachung am Arbeitsplatz**.



Dabei gilt es, ein Gleichgewicht zwischen der Privatsphäre der Mitarbeitenden und den berechtigten Interessen des Arbeitgebers, insbesondere der IT-Sicherheit, zu wahren. Voraussetzung ist eine klare und transparente Information über Nutzung, Kontrolle und Datenverarbeitung. Überwachungsmaßnahmen dürfen nur verhältnismäßig und abgestuft erfolgen.

Private Inhalte müssen eindeutig gekennzeichnet sein und bleiben geschützt, während angemessene technische Schutzmaßnahmen zulässig sind. Klare Regeln und Prozesse schaffen dabei die notwendige Rechtssicherheit.

Grundlage ist eine Praxis, die auf Transparenz, Verhältnismäßigkeit und Respekt der Privatsphäre beruht, wie von der CNPD - *Commission nationale pour la protection des données* empfohlen.

Welche Themen sind Ihnen wichtig ?

Die FGFC legt **großen Wert** darauf, die **Anliegen des Gemeindepersonals** ernst zu nehmen und ihre Kommunikation konsequent an Ihren Bedürfnissen auszurichten. Wenn Sie bestimmte Themen rund um die digitale Arbeitswelt besonders interessieren oder Fragen

haben, laden wir Sie herzlich ein, uns diese mitzuteilen. Ihre Rückmeldungen helfen uns, unsere Inhalte gezielt weiterzuentwickeln und praxisnah auf Ihre Erwartungen einzugehen.

Denn nur durch den direkten Austausch können wir sicherstellen, dass unsere Informationen und Weiterbildungsangebote den tatsächlichen Bedürfnissen des Gemeindepersonals entsprechen.

Euer FGFC-Team
Kontakt: fgfc@fgfc.lu

Thema 1

Cyberüberwachung am Arbeitsplatz

Basierend auf den Empfehlungen der CNPD (*Commission nationale pour la protection des données*)

1. Grundprinzip: Balance zwischen Interessen

Am Arbeitsplatz treffen zwei zentrale Interessen aufeinander:

- Privatsphäre der Mitarbeitenden (inkl. Schutz der Kommunikation).
- Schutzinteressen des Arbeitgebers (IT-Sicherheit, Vertraulichkeit, Funktionsfähigkeit).

Best Practices:

Ein ausgewogenes Verhältnis schaffen, das sowohl die Rechte der Mitarbeitenden respektiert als auch die legitimen Interessen des Unternehmens schützt.

2. Transparenz und Information

Der Arbeitgeber ist verpflichtet, Mitarbeitende klar und vorab über folgende Punkte zu informieren:

- erlaubte private Nutzung von IT-Systemen
- eingesetzte Überwachungsmaßnahmen.
- Zweck, Umfang und Art der Datenerhebung.

- Speicherdauer und Zugriff auf Daten
- mögliche Konsequenzen bei Verstößen.

Best Practices:

1. Einführung einer IT-Richtlinie / Nutzungsordnung (Charter).
2. Einbindung von Arbeitnehmervertretungen.
3. Leicht verständliche und zugängliche Kommunikation.

3. Verhältnismäßige und abgestufte Kontrolle

Überwachung darf nicht dauerhaft und pauschal erfolgen.

Best Practices

„Progressive Kontrolle“:

1. Erste Stufe: anonyme, allgemeine Auswertung (z. B. Nutzungsmuster).
2. Zweite Stufe: bei Auffälligkeiten gezielte Analyse.
3. Dritte Stufe: individualisierte Kontrolle nur bei begründetem Verdacht.

4. Umgang mit E-Mails

Grundsatz:

E-Mails gelten grundsätzlich als beruflich, außer sie sind als „privat“ gekennzeichnet.

Best Practices:

1. Private E-Mails klar kennzeichnen („privat“ im Betreff).
2. Trennung durch: separate Postfächer oder Ordner („persönlich“).
3. Arbeitgeber darf keine privaten E-Mails lesen (außer per Gerichtsbeschluss).
4. Abwesenheit von Mitarbeitenden
 - automatische Abwesenheitsnotiz einrichten
 - Vertretung festlegen
 - Zugriff nur auf notwendige berufliche Inhalte und möglichst in Anwesenheit eines Vertreters.

5. Internetnutzung

Internetzugang dient primär beruflichen Zwecken private Nutzung darf eingeschränkt werden.

Best Practices:

1. Klare Regeln zur Nutzung definieren
2. Zunächst anonyme Auswertung von Surfverhalten
3. Individuelle Kontrolle nur bei Auffälligkeiten
4. Präventive Maßnahmen:
 - Website-Filter
 - Download-Beschränkungen
 - Schutz vor Malware

6. Dateien und IT-Systeme

Grundsatz:

- Dateien sind grundsätzlich beruflich
- private Dateien müssen klar gekennzeichnet sein.

Best Practices:

1. Private Dateien in gekennzeichneten Ordnern speichern
2. Zugriff auf private Dateien nur:
 - mit Anwesenheit des Mitarbeitenden
 - oder mit dessen Möglichkeit zum Widerspruch
3. Sicherstellen, dass wichtige Unternehmensdaten auch ohne Zugriff auf private Ordner verfügbar sind.

7. Logging und technische Überwachung

- Logfiles und Nutzungsdaten dürfen erhoben werden,
- jedoch nur verhältnismäßig und schrittweise

Best Practice:

- Keine sofortige personenbezogene Auswertung – erst bei konkretem Anlass.

8. Offboarding (Austritt von Mitarbeitenden)

Best Practices:

1. Übergabe aller beruflichen Daten sicherstellen.
2. Private Daten dürfen kopiert und gelöscht werden
3. Konten nach Austritt deaktivieren.
4. Automatische Weiterleitung oder Information an externe Kontakte einrichten.

9. Datenschutzrechte der Mitarbeitenden

Mitarbeitende müssen jederzeit:

- Zugriff auf ihre Daten haben
- über Verarbeitungen informiert sein
- ihre Rechte ausüben können

Best Practice:

- Klare Prozesse für Auskunfts- und Löschanfragen definieren.

FAZIT CYBERÜBERWACHUNG

Eine rechtmäßige Cyberüberwachung am Arbeitsplatz basiert auf:

1. Transparenz
2. Verhältnismäßigkeit
3. Klaren Regeln
4. Respekt der Privatsphäre

Diese Regelungen sollten in enger Zusammenarbeit mit der jeweiligen Personaldelegation sowie dem Datenschutzbeauftragten (DPO) erarbeitet und umgesetzt werden.