finans förbundet



Monitored:
A report on privacy in the financial sector

Table of contents

Foreword: High time that monitoring issues were put on the agenda 3
Background 4
- Monitoring and stress 5
- Monitoring in the financial sector 6
- The purpose of monitoring 6
- Legal restrictions 7

About the survey 8
Results 9
- Registry extracts and background checks 9
- Drug tests 14
- Monitoring 17
- The degree of predictability 19
- Stress experienced as a result of monitoring 20
- AI-powered monitoring 22
- The view of the employer 24

Conclusions 27
- Widespread monitoring 27
- Monitoring causes stress 28
- A lack of knowledge 28
- High level of trust, but trust has its limits 29
- Consequences of monitoring for trade-union activities 29

Recommendations 30
- 1. Collaborate on privacy issues 30
- 2. Achieve greater transparency 31
- 3. Replace, limit, minimise 31
- 4. Promote trade-union privacy 32
- 5. Strengthen personal privacy protections 32



High time that monitoring issues were put on the agenda

Employees in the financial sector have been subjected to various types of monitoring for a long time. Many finance companies carry out security-sensitive activities and international legislation establishes requirements with regard to documenting certain communications and logging transactions.

At the same time, several types of monitoring have become widespread in working life. New technologies make it possible to collect more information on how work is carried out, though knowledge of how widespread these are in the financial sector has been limited up to now.

With this report, Finansförbundet (The Financial Sector Union of Sweden) aims to help gain a better understanding of how monitoring is used in the financial sector and how it is experienced by employees in that sector. Are employees aware of the extent of the monitoring that takes place? How does it affect the work environment? Are employees confident that the information collected is used responsibly? The results show that monitoring is common in the sector. Many employees understand that certain types of monitoring are necessary for reasons of security and compliance and most state that they trust their employer to manage the monitoring responsibly.

At the same time, the report shows that both employees and trade-union representatives often have limited insight into how monitoring works in practice. We are also able to identify a clear correlation between the amount of monitoring and the stress experienced.

It is therefore high time that employers and elected representatives put monitoring issues on the agenda. They need to work together to establish clarity concerning its purpose, scope and consequences to enable necessary security requirements to be combined with a sustainable working life and respect for personal privacy.



Camilla Linder
Chair of
Finansförbundet

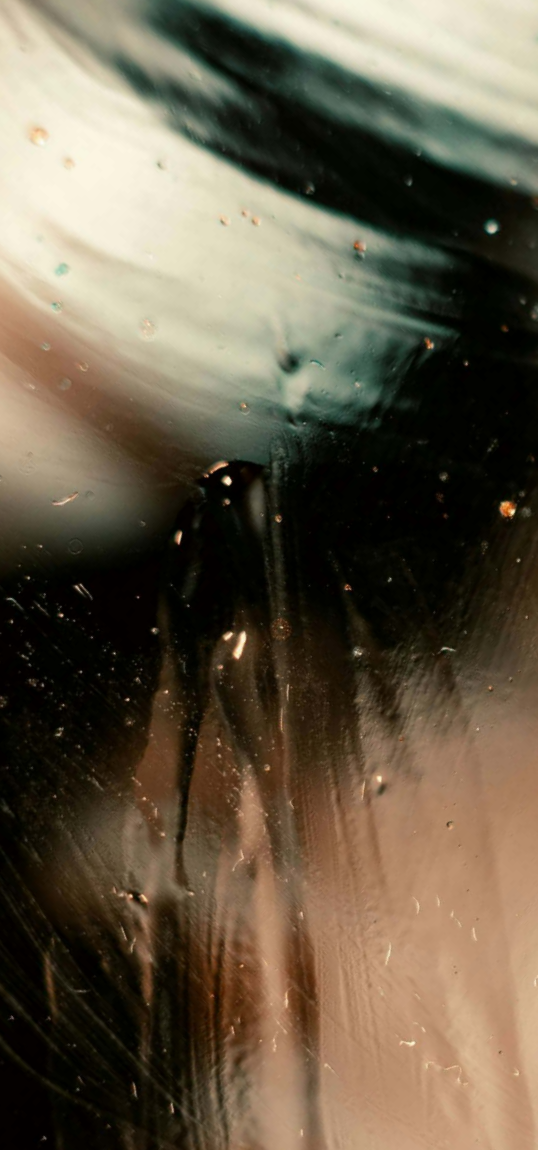
Background

Monitoring in working life is nothing new. Work has always been subjected to various types of measurement and checks. However, technological advances have made it easier to monitor more highly-qualified white-collar occupations.

In principle, all activity taking place in companies' IT systems can now be monitored and recorded. And while interception and analysis of digital communications has previously involved time-consuming manual work, new AI technologies are making monitoring cheaper and enabling it to be carried out on a larger scale.[1] A number of international reports actually do point out that monitoring of employees has increased, particularly in service- and knowledge-intensive occupations.[2]

In addition to direct monitoring of day-to-day work, there are also other ways of collecting information and surveying employees for security purposes or for assessing their suitability for the work. In Sweden, it is possible to identify a clear increase in background checks in the form of extracts from police criminal records during recruitment.[3] An increase in employer requests for employees to submit drug tests in order to verify that employees are not under the influence of drugs can also be identified.[4] These activities contribute to the overall amount of monitoring experienced by employees.

The rise of AI is also making it easier for employers to process large amounts of collected information, analyse performance, and evaluate work. There is also a risk of employees experiencing greater alienation when performance is assessed by AI instead of by a manager with whom it is possible to have a live conversation. For these reasons, it is becoming more and more relevant to gain an understanding of how monitoring is now used and how it is experienced by employees.



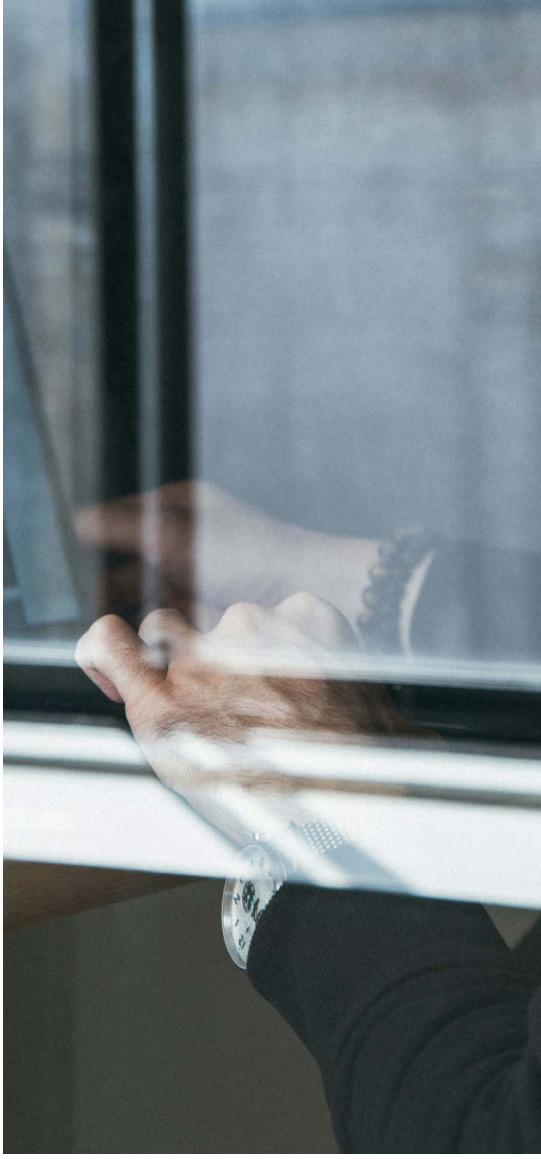
Monitoring and stress

There is clear evidence that monitoring affects employee well-being and stress. Multiple sources support the existence of such a correlation. The European Commission Joint Research Centre has concluded that:

> *Excessive monitoring has negative psycho-social consequences including increased resistance, decreased job satisfaction, increased stress, decreased organisational commitment and increased turnover propensity.*[5]

The correlation has also been established specifically in the financial sector when digital monitoring of performance is perceived to be excessive. It reduces trust and leads to greater anxiety as well as a perception of loss of control.[6] However, the researchers do not simply describe monitoring as bad from a one-sided perspective, but also state that monitoring can sometimes lead to improved performance.

Nevertheless, the purpose of the monitoring does affect the employees' perception of it. In general, most people appear to accept monitoring for security reasons, whereas there is greater resistance to monitoring that is perceived as excessive or that does not have a clear purpose. The effects of monitoring for the purpose of assessing performance may differ according to how it is used: It has a more negative effect if the employees experience monitoring as a form of control whereby mistakes risk leading to various types of punishment. If, on the other hand, employees feel that the monitoring is being used constructively as part of a learning process, it can have positive effects. Furthermore, it is possible to identify a greater negative effect when monitoring focuses on individual outcomes, whereas monitoring at group level is not felt to be so stressful.[7]



Monitoring in the financial sector

Since the financial sector's activities are security-sensitive, there are express requirements for monitoring in order to prevent and/or detect irregularities. For example, the EU MiFID II regulations contain requirements for certain telephone conversations and digital communications with customers and other operators to be recorded.[8] There are also requirements for background checks under the Security Protection Act. However, these requirements are confined to banks that carry on security-sensitive activities, such as systemically important banks. They also do not include all employees, but only persons who participate in security-sensitive activities or who have access to classified information.

According to Finansarbetsgivarna (The Employers of the Financial Sector), many banks now use drug tests as part of the recruitment process. In early 2026, the organisation also called on its member companies to increase the use of random drug testing during ongoing employment.

There are signs that monitoring in the financial sector has increased in recent years and that its scope extends beyond the statutory requirements.[9] However, examples that can be substantiated come from other countries and knowledge of monitoring in the Swedish financial sector is limited.

The purpose of monitoring

Information on employees may be collected for several possible purposes, the most common of which are security and to check or assess employees' work performance.

Security measures may, for example, be aimed at identifying insiders or enablers, who are a permanent threat in the banks.[10] Various forms of background checks and registry extracts are often used to capture these individuals, for example checks carried out at the time of new employment to checkwhether the person has been convicted of a crime. Drug tests are also sometimes justified with reference to the fact that people who buy drugs risk ending up in a dependent relationship with criminals.

However, monitoring is often aimed at measuring and evaluating employees' work performance. This may involve recording logins to see how much work an employee does[11] or using location data to check the employee's physical location.

An intervention may sometimes take place for several possible purposes: Recording a phone call can be a reassuring security measure that makes it possible to go back and show what was said in a conversation with a customer. It can also be used by managers to assess how an employee is doing their job or to enable new employees to listen in to conversations for training purposes.

Legal restrictions

Monitoring is usually a form of processing of personal data. Any information that can be linked to a person constitutes personal data. This includes, for example, emails, phone calls, video recordings and performance logs at an individual level. All personal data management needs to be supported by the General Data Protection Regulation (GDPR).

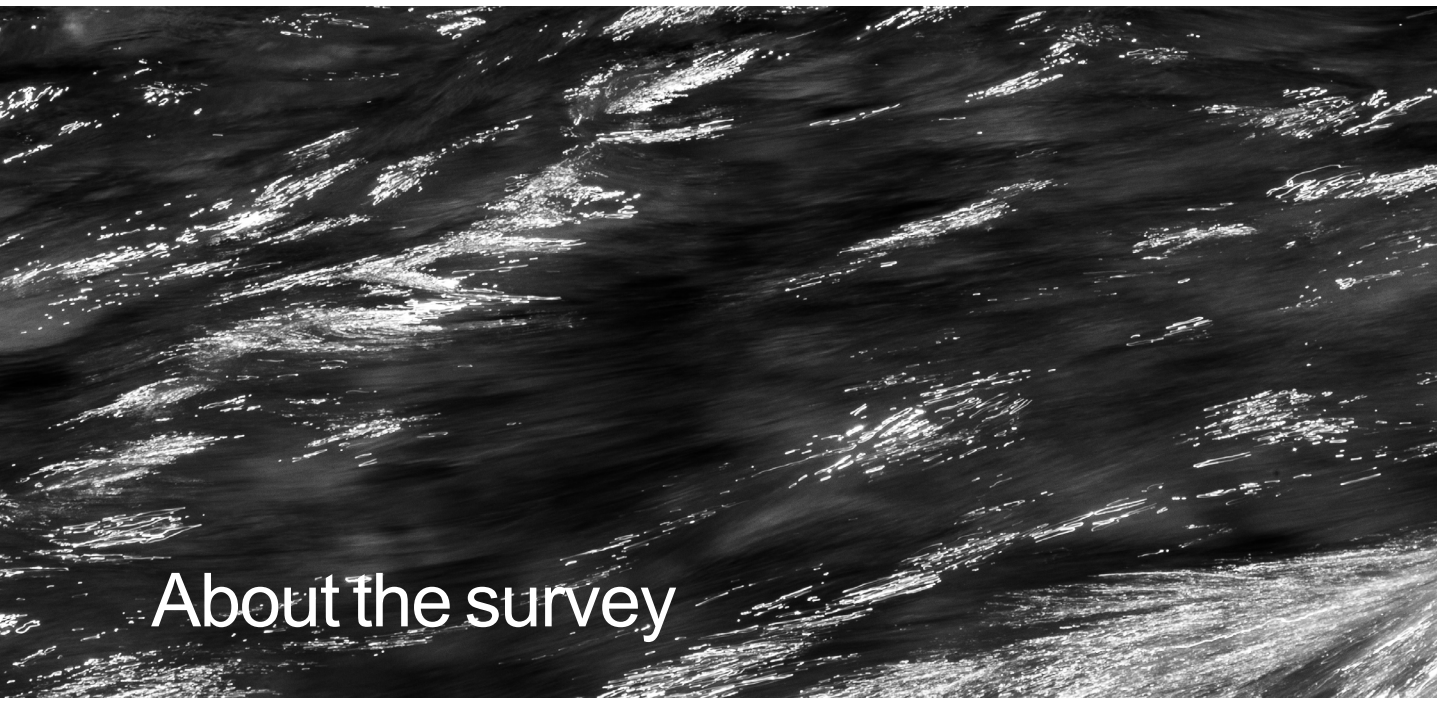
According to the General Data Protection Regulation, the person processing the personal data needs to clarify the purpose of the processing. There must also be a clear legal basis and the processing needs to be proportionate to the extent to which personal privacy is restricted. The legal basis may consist, for example, of the employer's legitimate interest in detecting IT security threats or preventing unauthorised access to information, provided it is not outweighed by the employees' interest in privacy. However, the legal basis of consent is rarely valid in the case of an employee, as there is a relationship of dependency between the employer and the employee.[12]

Furthermore, there is a requirement for data minimisation: The employer must not collect more personal data than is necessary or store it for longer than is necessary. Overall, that means that the processing of personal data must not be arbitrary, but must always have a legitimate purpose.[13] In addition, the use must be limited to the purposes for which the data was collected. If, for example, camera surveillance is carried out for the purpose of preventing crime, the recordings must not be used to check up on the length of employees' breaks.

Finally, the person being monitored has a right to information on what data is being collected, for what purpose and how it is used. This mainly consists of two requirements: an obligation to inform prior to or during the processing of the personal data and a right for employees to request an extract of the personal data processed by the employer.

However, the GDPR is not the only restriction on the way in which employers are able to monitor employees or collect and process personal data. The EU AI Regulation imposes restrictions on the way in which employers are able to use AI in recruitment, distribution of work or assessment of employee performance, for example. Employers must ensure that people are always involved in decision-making and must also inform the employees concerned that AI systems are being used to support those processes. The AI Regulation therefore restricts how the data is subsequently used rather than what data can be collected.

With regard to drug tests, a judgment of the Labour Court also specifies three situations in which a test may be justified: If the performance of the work is dangerous or unlawful, if the work is particularly security-sensitive or if, due to the particular nature of the activity, the employer must be able to prove that the employees are drug-free.[14] This is not a definitive list, but can be used as a starting point and must be weighed against the employee's interest in maintaining personal privacy.

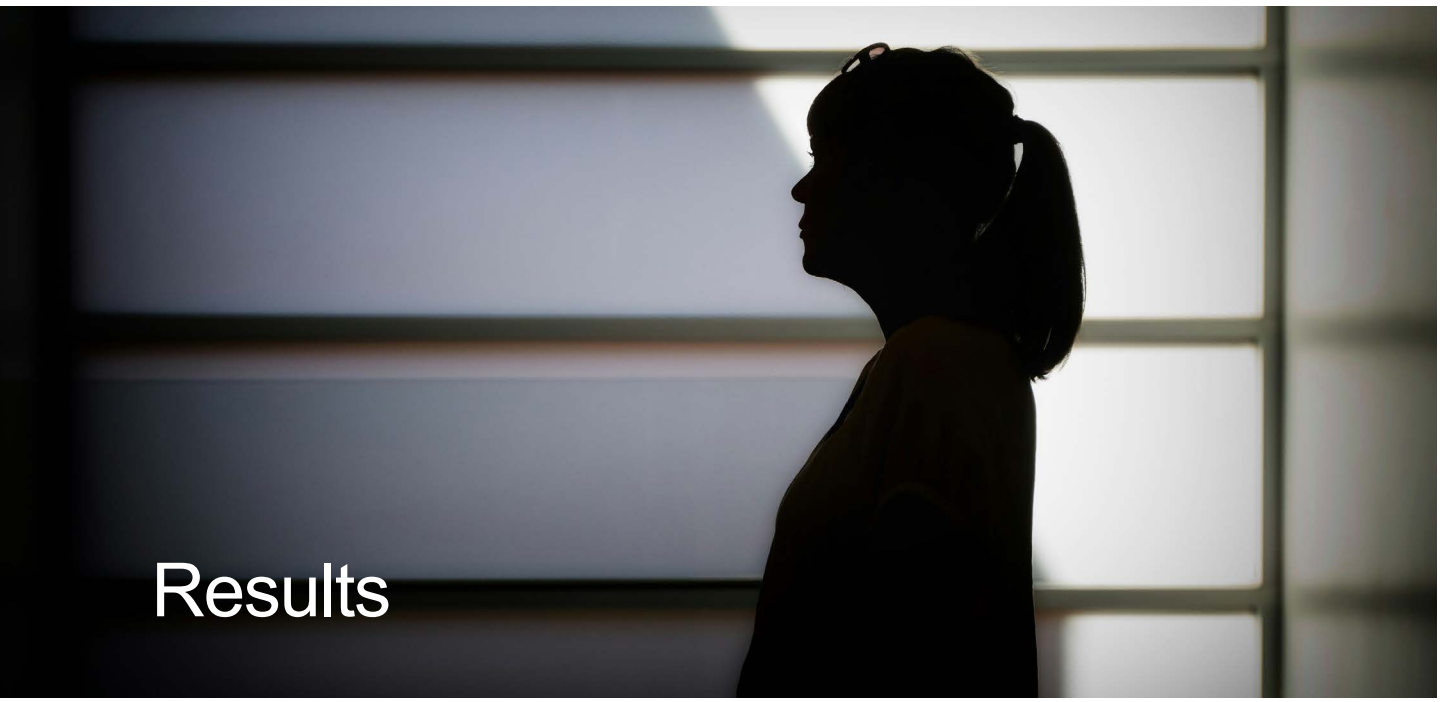


About the survey

This report is based on a survey that Finansförbundet sent out to its members. The survey was divided into three themes addressing different aspects of employees' privacy: Background checks, drug tests and monitoring. The survey also included a theme on AI use, which has been reported on separately by Finansförbundet in another report.

The survey was open from 19 May to 2 June. 1,421 people responded to it. All respondents are or have recently been employed in the financial sector.

The response rate is 5.7%. The respondents correspond to the membership group as far as gender and professional roles are concerned. However, there was a higher proportion of older respondents. The responses are therefore weighted according to age. The results therefore reflect the membership group in terms of age, gender and professional roles. That means that the survey provides a proportionately representative view of the situation in the financial sector.



Results

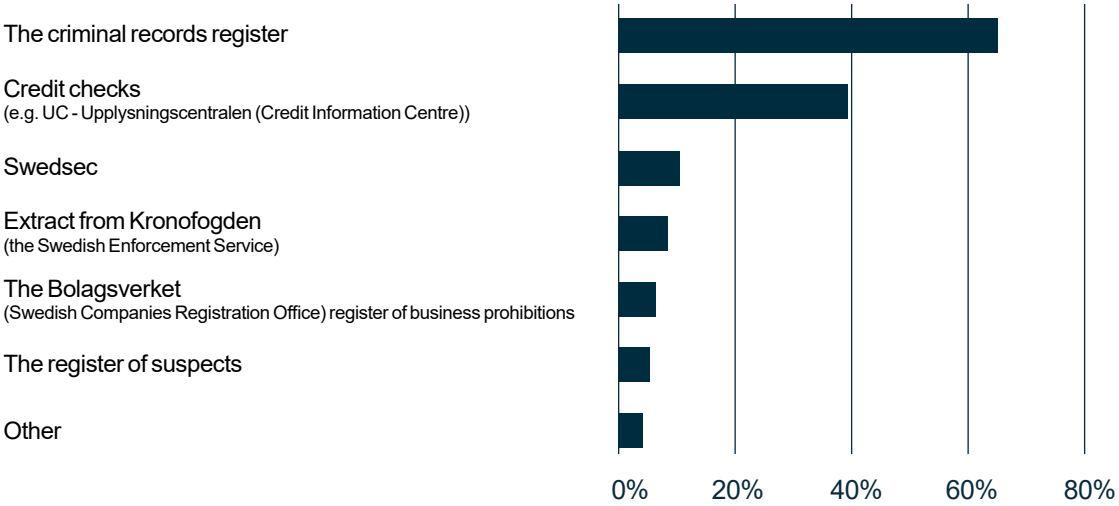
Registry extracts and background checks

The survey responses show that background checks are relatively common in the financial sector. 68 per cent have needed to submit registry extracts to their employer at some point. 15 per cent answer that their employer has not requested extracts from any of the registers specified in the survey. A further 17 per cent answer that they do not know.

”[The bank] has become insanely monitored to the point where people don’t dare leave their work station to go to the toilet. I feel constantly monitored by my boss.”

From the free-text responses

“Has your current or most recent employer ever requested extracts from any of the following registers?”





Extracts from the criminal records register are the most common (65 per cent). Since a total of 68 per cent have provided some form of registry extract, that means that almost everyone who needs to provide some registry extract has needed to provide an extract from the criminal records register: only 3 per cent have needed to provide an extract from other registers without also providing an extract from the criminal records register.

Extracts from the criminal records register are most common among employees in advisory services (81 per cent) and least common in IT and data analysis (55 per cent).

The second most common is for the employer to carry out a credit check (39 per cent). This is also most common among employees in advisory services (47 per cent). It is least common among employees in capital markets (32 per cent).

Only 10 per cent answer that their employer has requested an extract from Swedsec. Among employees in advisory services, that figure is only 20 per cent. It is an unexpectedly low figure: A Swedsec licence is often a requirement for working with classified information in banking and finance and there are a total of 24,000 active licences, which corresponds to more than half of all bank employees.[15] The employer must also continuously check that the employees concerned have a valid licence. However, the employer can carry out this check directly with Swedsec, which means that the employees are not directly involved. One explanation for the low figure could therefore be that the employees do not notice when the employer carries out the check or that they do not consider it to be a registry extract.

Other registry extracts are relatively rare. 8 per cent have needed to provide an extract from Kronofogden, 6 per cent from the Bolagverket register of business prohibitions and 5 per cent from the police register of suspects.

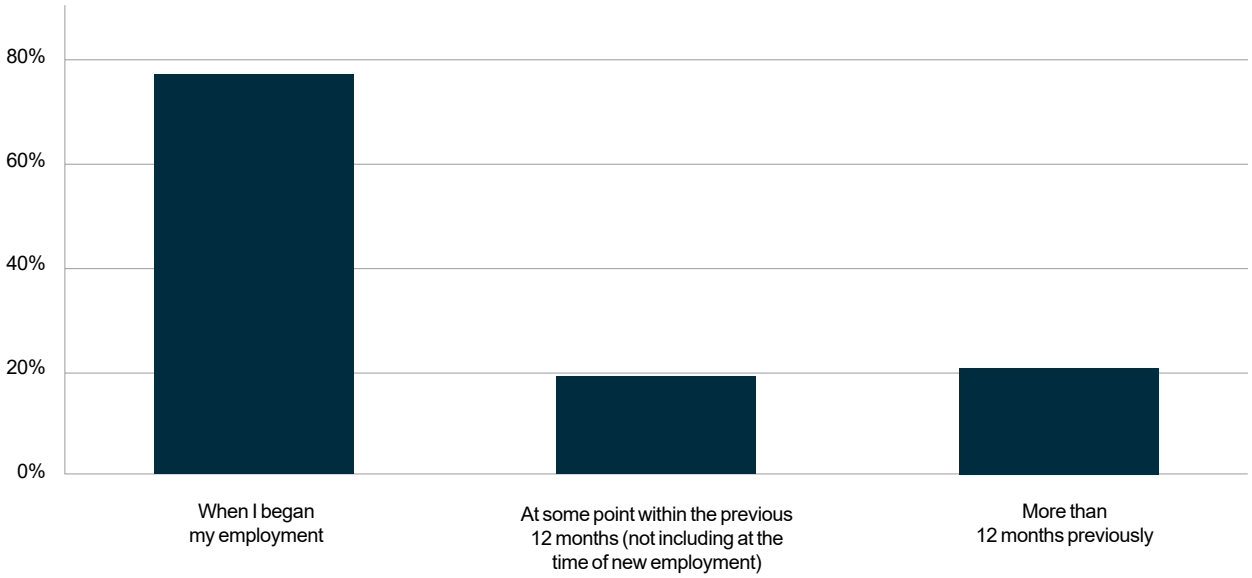
There are some differences according to the category of employer. Among employees at savings banks, 85 per cent have needed to provide an extract from the criminal records register and 63 per cent from the police register of suspects.

More common in the case of new employment

Among those whose employer has requested an extract from the criminal records register, 77 per cent state that this took place at the time of new employment. For 19 per cent, the employer requested an extract during ongoing employment in the previous 12 months, whereas 21 per cent answer that the request was made during ongoing employment more than 12 months previously.

The same question was asked regarding the register of suspects. The picture is basically the same: 74 per cent answer that the extract was requested at the time of new employment, 20 per cent during ongoing employment in the previous 12 months, and 21 per cent during ongoing employment more than 12 months previously. However, please note that this distribution refers to significantly fewer respondents since extracts from the register of suspects are uncommon.

"When was an extract from the criminal records register/the register of suspects requested?"



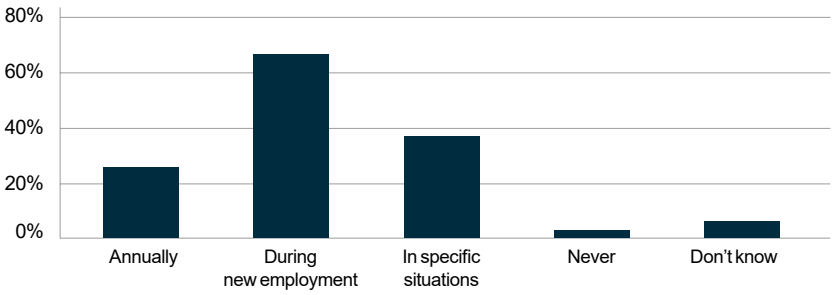
Clear age differences

There is a clear age difference when it comes to experience of registry extracts. It is more common for employees aged 34 or below to answer that their employer has requested an extract from the criminal records register (74 per cent) or carried out a credit check (49 per cent). The corresponding figures for employees aged 55 or over are significantly lower (52 per cent for the criminal records register, 25 per cent for credit checks). This is probably related to the fact that most registry extracts are requested at the time of new employment and younger people have been employed for a shorter time, in combination with the fact that background checks have become more common in recent years.

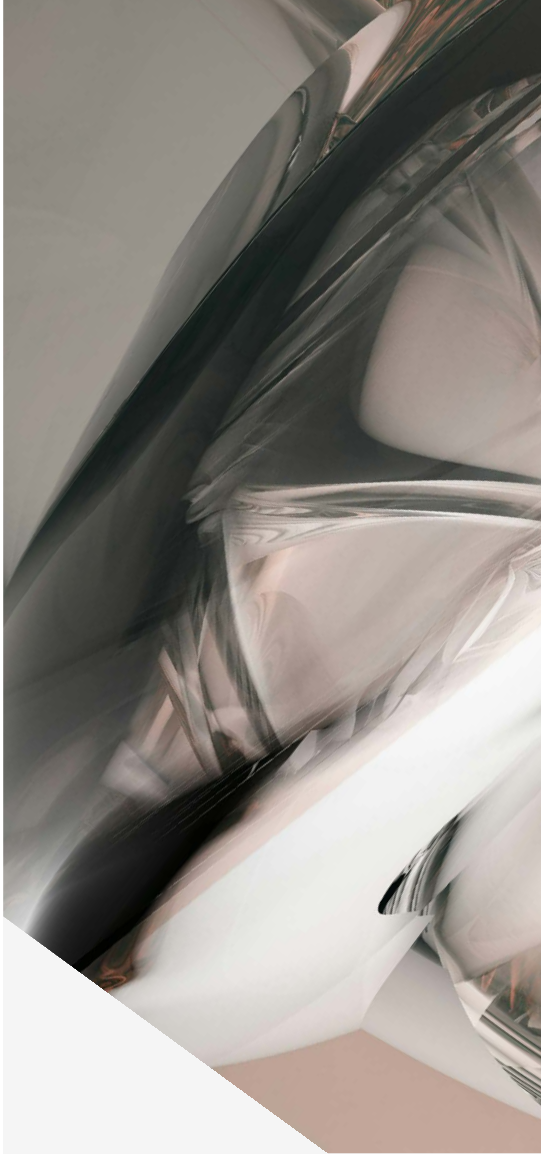
Acceptance of certain registry extracts at the time of new employment

Many employees think it is reasonable for the employer to carry out certain background checks. 65 per cent consider that the employer should request an extract from the criminal records register at the time of new employment. However, significantly fewer support the idea of requesting these extracts during ongoing employment either annually (24 per cent) or in specific situations (36 per cent). However, only 3 per cent consider that checks of that kind should never take place.

"When do you think the employer should ask someone to provide an extract from the criminal records register?"

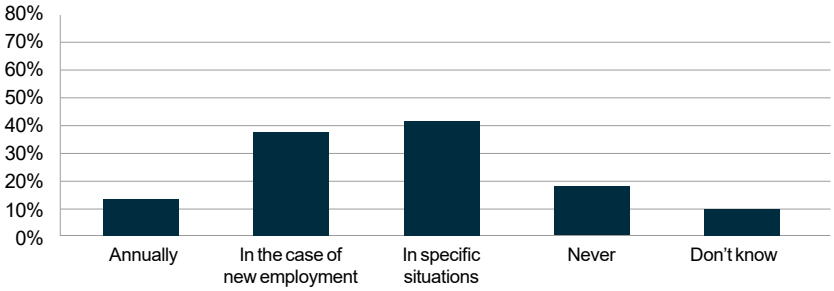




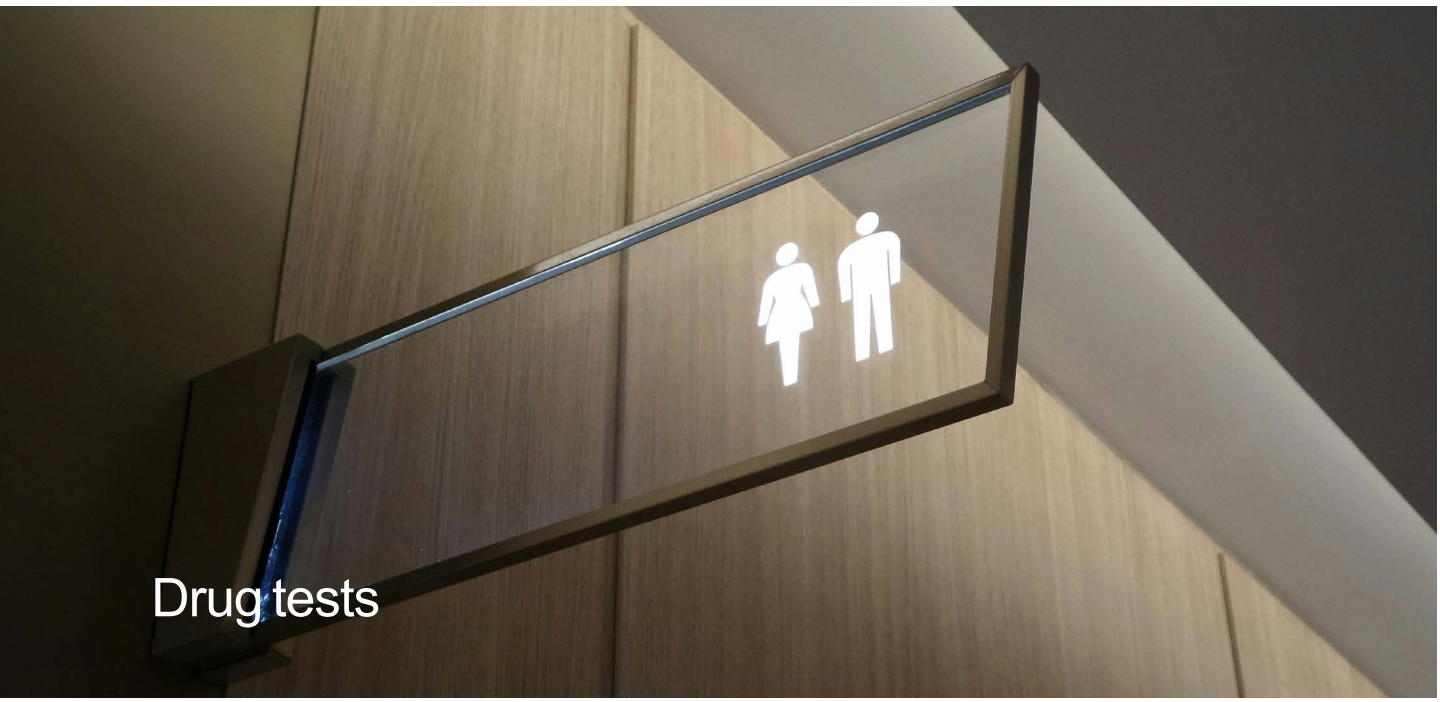


For credit checks, which are the second most common form of registry extracts, 37 per cent consider that employers should carry out a check at the time of new employment. Only 13 per cent consider that the employer should carry out such a check annually. However, slightly more (42 per cent) believe that such a check should take place in specific situations. Employees who have themselves been subjected to a credit check have a more positive attitude, whereas those who have not been subjected to a credit check are more negative. A total of 18 per cent consider that such a check should never take place.

"When do you think the employer should ask someone in your professional role to provide credit information (e.g. UC)?"



The results for other registry extracts follow roughly the same pattern as for credit checks: Almost half consider that the employer should request extracts from the police register of suspects, Kronofogden or the Bolagsverket register of business prohibitions in specific situations. Fewer consider that they should be requested at the time of new employment and only a small proportion consider that they should be requested annually. Around 15 per cent consider that the employer should never carry out these checks.



Drug tests

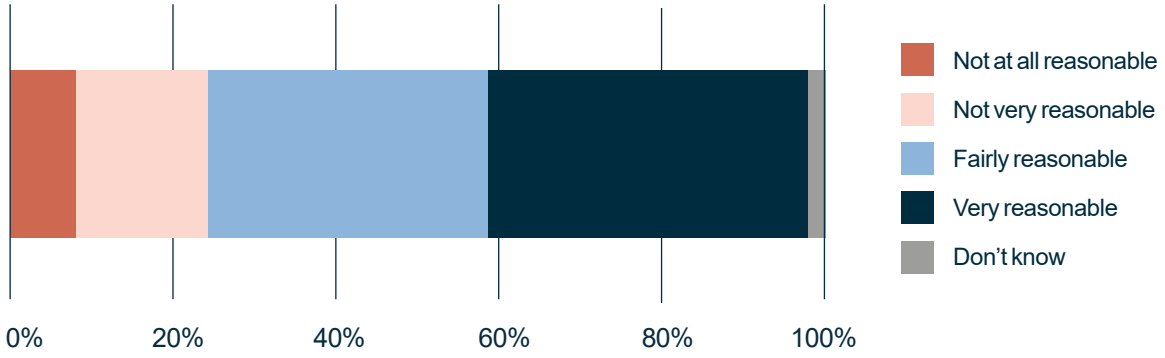
The survey responses show that there is a relatively high acceptance of drug tests, even though in practice they are still relatively uncommon and mainly occur at the time of new employment.

The majority of employees (73 per cent) consider it reasonable for employers to carry out drug tests. 24 per cent do not consider it reasonable.

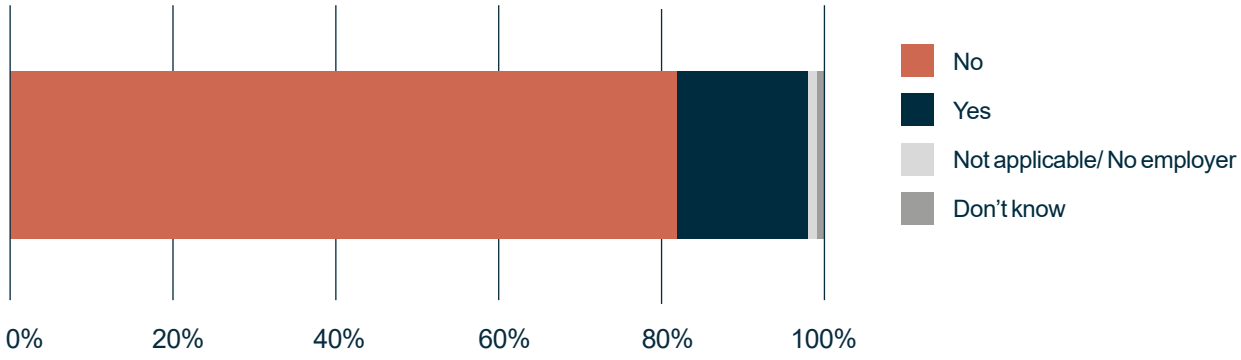
Most have no personal experience of submitting drug tests. 82 per cent answer that they have not submitted a drug test to their employer, whereas 16 per cent answer that they have. This corresponds to 184 respondents (unweighted).

There are clear differences between the banks. Drug testing is uncommon at some major banks, whereas it occurs to a significant extent at others.

"To what extent do you think it is reasonable for employers to carry out drug tests?"

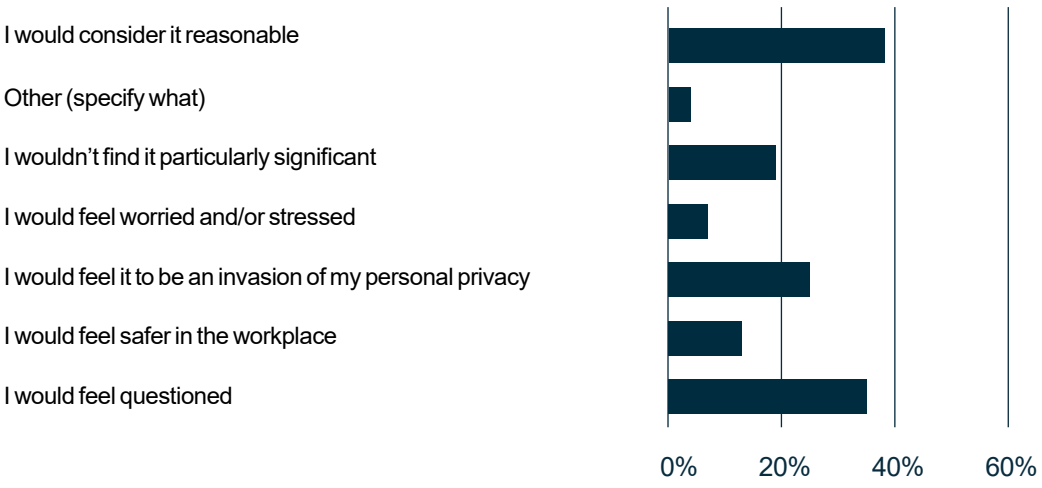


"Have you submitted a drug test during your employment?"



Of those who have submitted a drug test, 85 per cent state that it took place at the time of new employment. A few state that it was linked to routine procedures, a specific event or random checks, but those responses represent only around 1 per cent of all respondents. The survey also included a question on the appropriate consequences if the drug test proved positive. The most common response was Don't know (52 per cent), followed by Contact with occupational health care (23 per cent), Dismissal (22 per cent) and Offer of rehabilitation (21 per cent). Those who had not themselves submitted a drug test were asked how they would feel if their employer requested one. 38 per cent would consider it reasonable, whereas 35 per cent would feel questioned and 25 per cent would consider it an invasion of personal privacy. 13 per cent would feel safer in the workplace. Only 7 per cent state that they would feel worried and/or stressed. 19 per cent would not find it particularly significant.

"How do you think you would feel if your employer asked you to take a drug test during ongoing employment?"

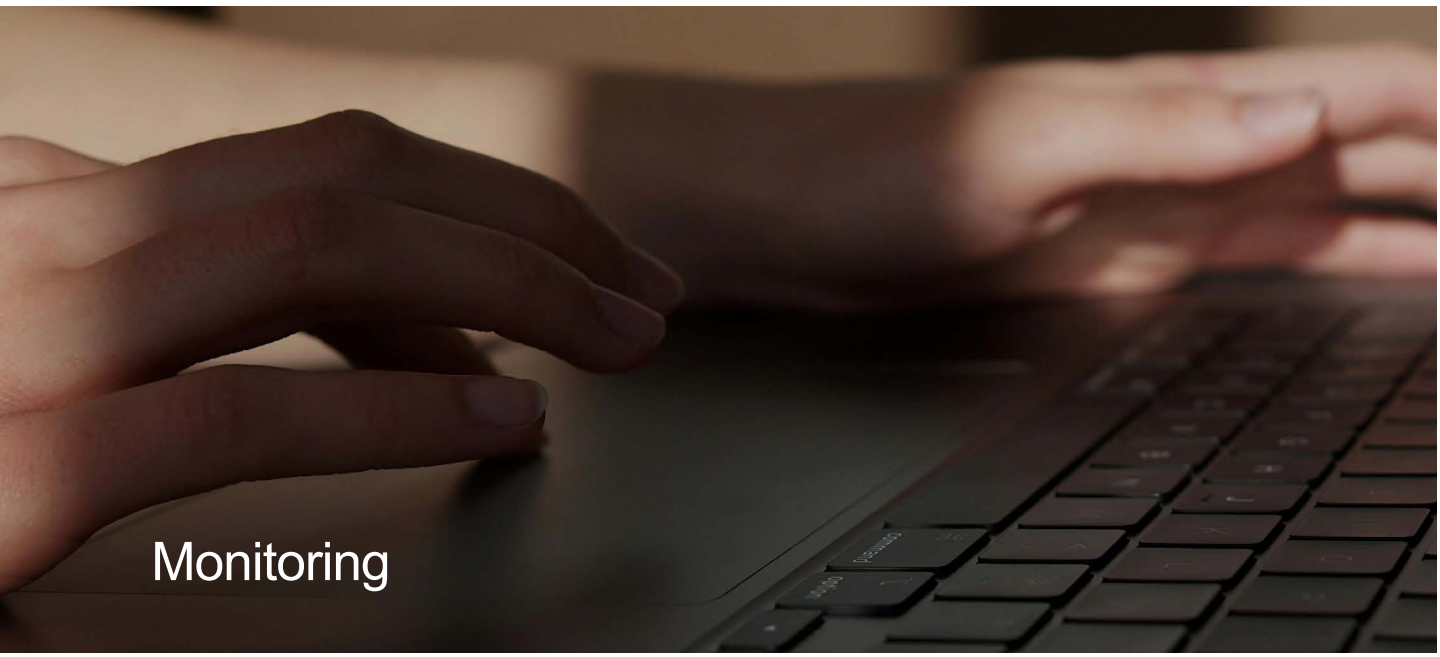


Employees who take medication

The survey included a question about whether respondents themselves took prescription medication that could register during a drug test. 5 per cent answered “Yes” to this question.

Within this group, however, attitudes to drug testing differ significantly from those of other employees. 47 per cent of this group would feel questioned if their employer requested a drug test, and 37 per cent would consider it an invasion of their personal privacy. Only 24 per cent would consider it reasonable. The differences between the groups are relatively large and are statistically significant. The differences for the other response options were not statistically significant.



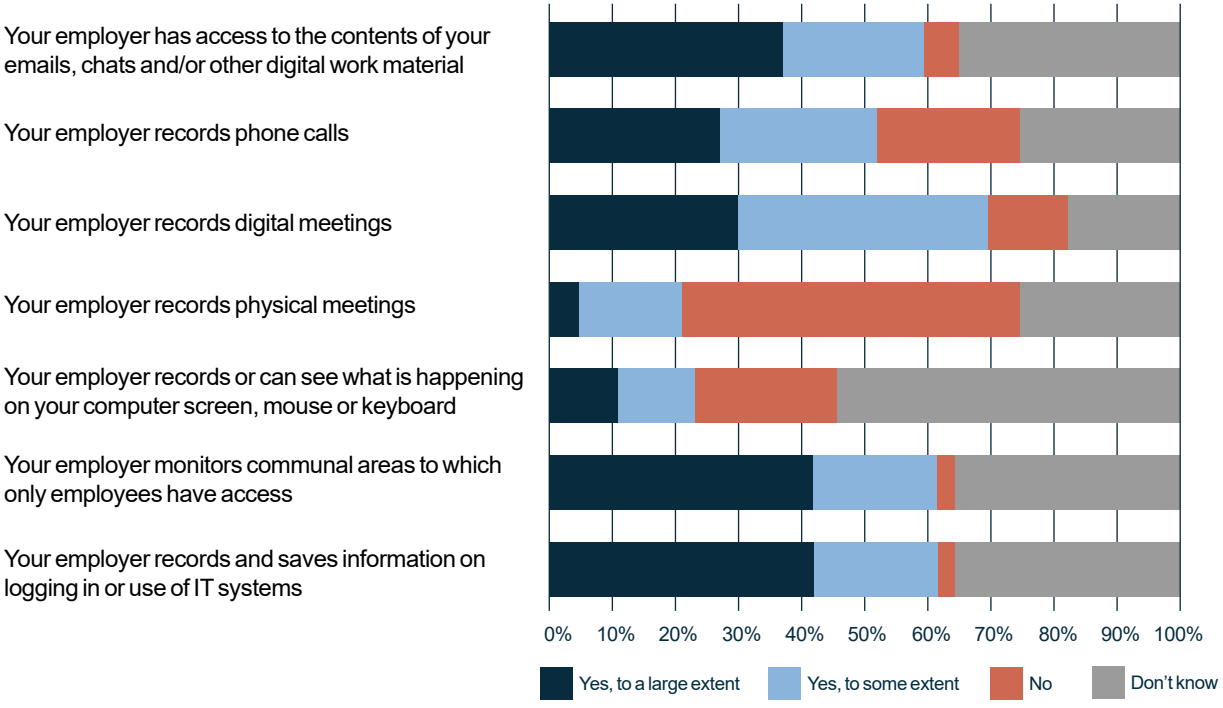


Monitoring

The survey included questions on the extent to which the respondents have experience of seven types of monitoring. The most common type of monitoring appears to be recording of digital meetings by the employer (70 per cent, followed by camera surveillance (62 per cent) and recording and saving by the employer of information on logins or use of IT systems (62 per cent).

59 per cent state that their employer has access to employees' emails, chats and/or other digital work material. Only 6 per cent answer that their employer has no access to that material. The remaining 35 per cent state that they don't know.

Experiences of monitoring



In theory, most employers are likely to have access to digital work material because they normally own email systems and employees' user accounts. An IT administrator with the right permissions can basically access all material. The result may be a reflection of the fact that employees are aware of this. This in itself does not necessarily mean that employers regularly and actively access employees' communications.

52 per cent state that their employer records phone calls. This is most common in customer services, where 81 per cent answer that phone calls are recorded. It is even more common for conversations to be recorded in advisory services (73 per cent) and capital markets (77 per cent).

70 per cent state that their employer records digital meetings (with audio and/or video or saved transcripts). This is the most common type of monitoring in the survey. As with recording of phone calls, recording of digital meetings is more common among employees in customer services (80 per cent), advisory services (83 per cent), and capital markets (72 per cent). They also more commonly answer that such recording takes place to a large extent. Many employees in other professional roles also state that such recordings take place, but most answer that it takes place to some extent.

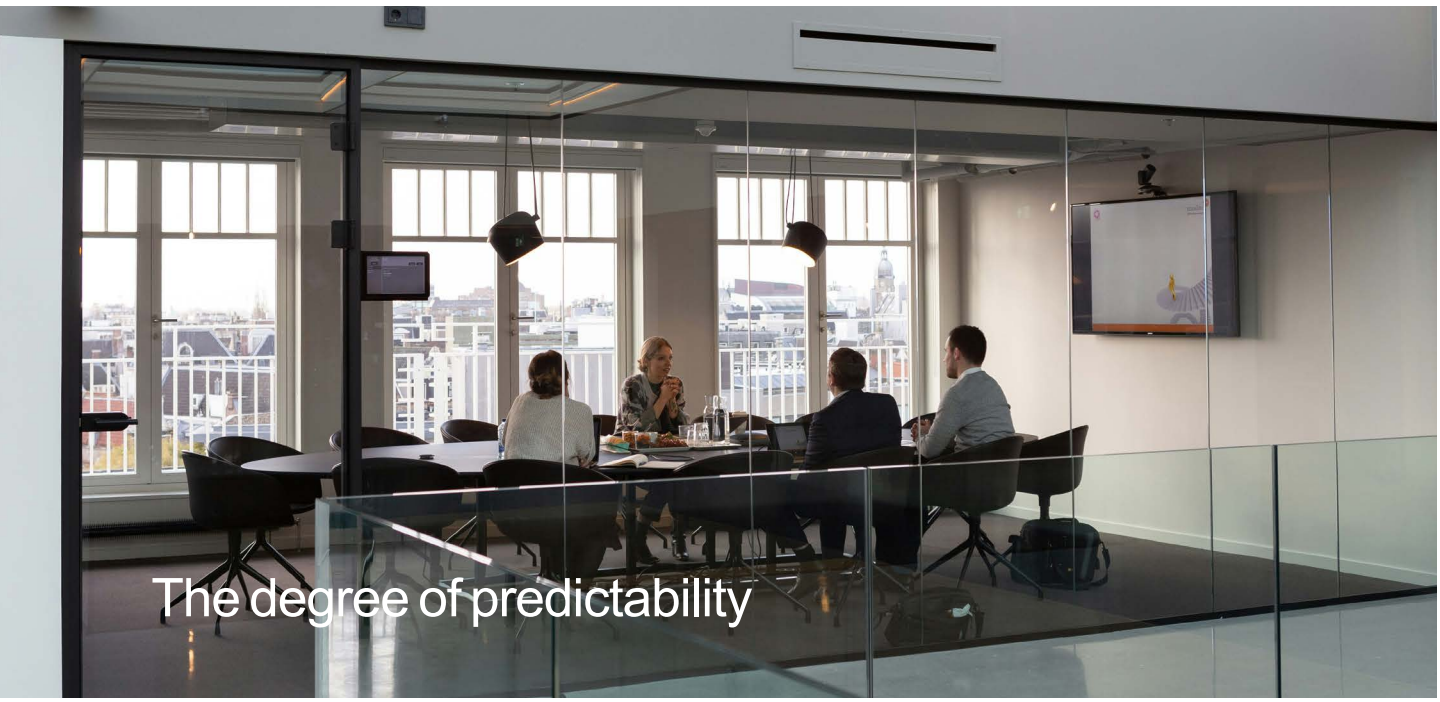
21 per cent state that their employer records physical meetings (with audio and/or video or saves transcripts). Only 5 per cent state that it occurs to a large extent. In general, this is the least common type of monitoring in the survey. It is slightly more common in customer services (29 per cent overall) and less common in advisory services (14 per cent overall).

23 per cent state that their employer records or can see what is happening on their computer screen, mouse or keyboard. However, 54 per cent answer that they do not know, which stands out from other questions in the survey.

62 per cent state that their employer monitors communal areas, meeting rooms, break rooms or other spaces to which only employees have access. This occurs more often at the major banks (63 per cent) than at other companies (around 57 per cent).

62 per cent state that their employer records and saves information on logins or use of IT systems (e.g. Teams, history from the use of AI tools, company-specific systems, etc.). Most state that this occurs to a large extent (42 per cent).

Elected representatives have slightly more knowledge than other employees: On average, 35 per cent of employees answer that they do not know what types of monitoring occur, whereas only 25 per cent of the elected representatives answer that they do not know.



The degree of predictability

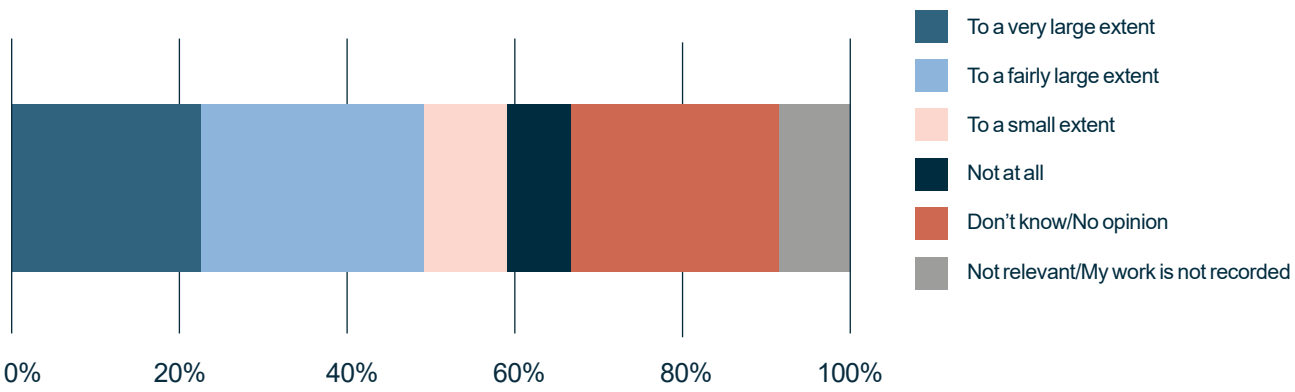
Employees must be informed of when they are being monitored and how. Not knowing whether or when work is being recorded can in practice feel as stressful as being monitored all the time. Sometimes the uncertainty can be enough for an employee to refrain from taking short breaks or going to the toilet.

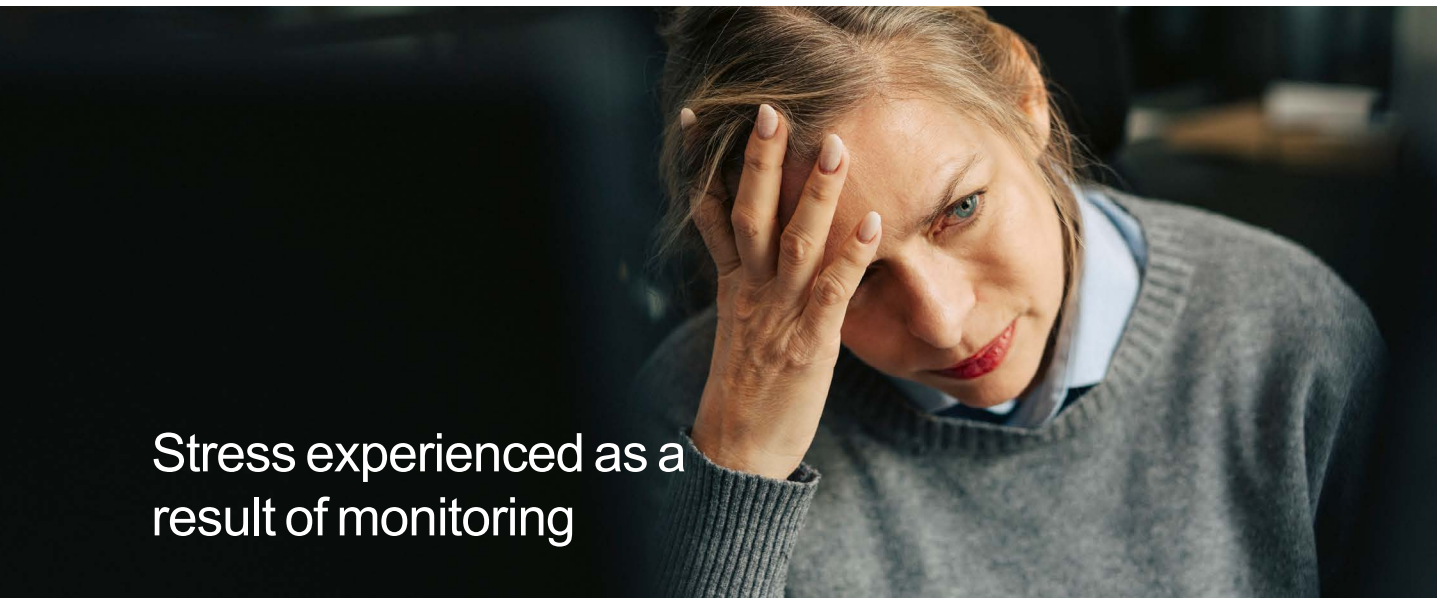
49 per cent state that they can predict when their work will be recorded. 17 per cent answer that they cannot predict it and 25 per cent answer that they do not know. 9 per cent state that the question is not relevant/that their work is not recorded.

"I have no problem with monitoring or checks. However, the important thing is for the employer to be open and to inform employees about what is being monitored/ checked and how it is then used. Full transparency!"

From the free-text responses

"Can you predict when your work might be recorded?"



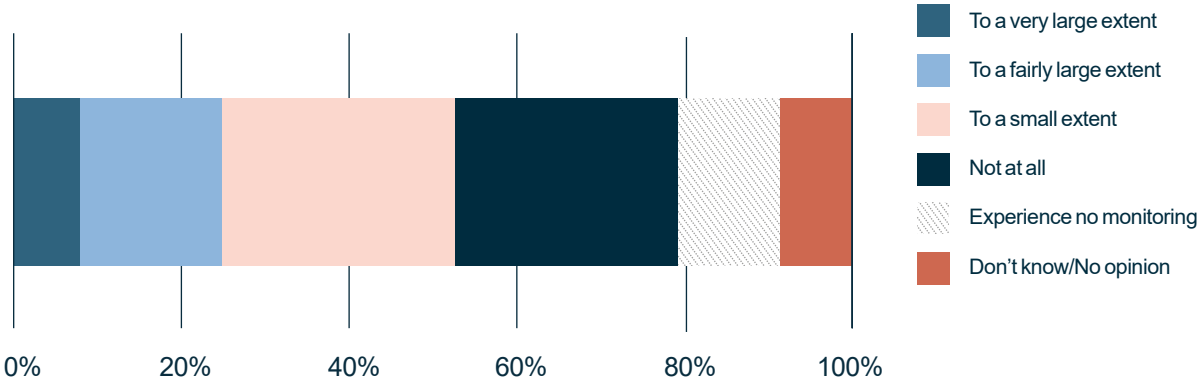


Stress experienced as a result of monitoring

25 per cent state that they are more stressed as a result of monitoring at work. The figure is significantly higher (41 per cent) in customer services, but it is also higher than average for advisory services and asset management (both at 32 per cent). However, in the categories of regulatory compliance, IT and data analysis and business support, the response that they did not experience any monitoring (15 per cent, compared to around 5 per cent in the more customer-oriented roles) was more common.

Several free-text responses address the correlation between monitoring and performance requirements and the fact that it is felt to be particular stressful when work is constantly measured. Some free-text responses also highlight how managers monitor schedules and booking systems so there are unlikely to be any gaps in the schedule, which can mean that a fast pace is constantly maintained. Some answers also describe how monitoring causes greater fear of making mistakes, which reduces motivation. The number of free-text responses is insufficient to allow any statistical conclusion to be drawn, but it can still provide a more concrete insight into the ways in which monitoring causes stress in the financial sector in particular.

"To what extent do you experience greater stress as a result of monitoring in your work?"



Strong correlation between monitoring and stress

As mentioned in the background section, the research contains evidence of a correlation between monitoring and stress. To better understand this correlation, we have investigated the relationship in the survey responses between total amount of monitoring and perceived stress. This is interesting because it is not necessarily a particular type of monitoring but rather the aggregate amount that affects the overall experience.

To carry out this comparison, we have compiled a weighted index of the seven types of monitoring included under the heading of Monitoring. The index varies between 0 and 100, with 0 indicating that the respondent does not experience any type of monitoring and 100 indicating that the respondent experiences all types of monitoring to a large extent. The average value is 58.

Perceived stress	Monitoring index
Experiences no monitoring	37,0
Not at all	53,1
To a small extent	59,7
To a fairly large extent	68,0
To an extremely large extent	76,1

As can be seen from the table above, there is a clear correlation between monitoring and perceived stress. Those who do not feel that monitoring causes greater stress are less likely to be subjected to monitoring (53.1 on the index). The respondents who consider that monitoring causes greater stress to a very large extent also experience significantly more monitoring (76.1). The differences in the monitoring index between people with different levels of perceived stress are statistically significant. The effect is considerable, which shows that there is a clear correlation between perceived monitoring and stress.

Monitoring of communications (emails, chats, phone calls and meetings) has a particular correlation with stress. Camera surveillance, on the other hand, has no clear association. This is consistent with other research which has shown that monitoring causes more stress when it can be used to assess employees' work performance rather than for purely security purposes. Of course, recordings can also be used as a security mechanism, for example to enable clients who are guilty of threats and harassment to be prosecuted, but if this was really felt to be the primary purpose, the recordings should lead to less rather than more stress.

There is also a correlation between perceived stress and inability to predict when recording will take place.

"My employer compiles statistics on how many tasks we do, how long they take and how much 'other' time we have and then follows up on it on a monthly basis. There are also set goals for the average number of cases we deal with per month. This is felt to be extremely stressful."

From the free-text answers

Table: Monitoring and perceived stress. The table shows the average value of the monitoring index divided according to how the respondents feel that monitoring affects their stress levels.



AI-powered monitoring

One important issue from a privacy point of view is how employers then process the information they collect on employees. In recent years, the use of AI tools has become increasingly common in working life. AI is often used by the employees themselves, though it is occasionally also used by employers as a personnel management tool, to monitor or assess employees' work. Use of AI as apersonnel management tool normally requires data on the employees. This can consist of statistics, logs, recordings, background information, etc. There is thus a potential correlation between the level of monitoring in day-to-day work and the prerequisites for using AI tools to assess employees' work.

71 per cent state that they do not know whether their employer uses AI tools to process and/or analyse recordings relating to their work. Among the remainder, slightly more answer "Yes" (16 per cent) than "No" (14 per cent). However, more people (28 per cent) answer "Yes" in customer services in particular and more people (23 per cent) in advisory services state that their employer uses AI in this way.

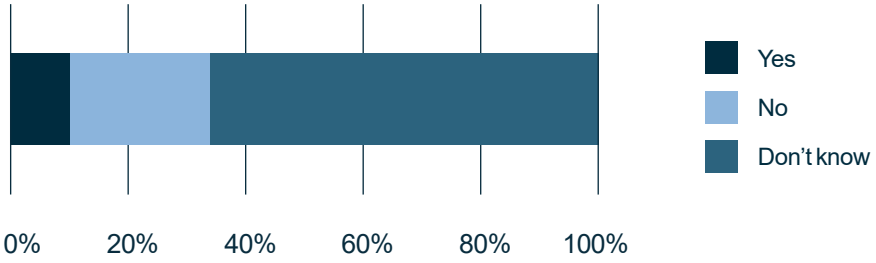
66 per cent state that they do not know whether their employer uses AI tools to measure or assess their performance. 24 per cent answer "No" to this question and only 10 per cent answer "Yes". In customer services, the proportion of respondents answering "Yes" is more than twice as high (27 per cent) and it is also slightly higher in advisory services (16 per cent).

"It results in me losing motivation and trust in my employer."

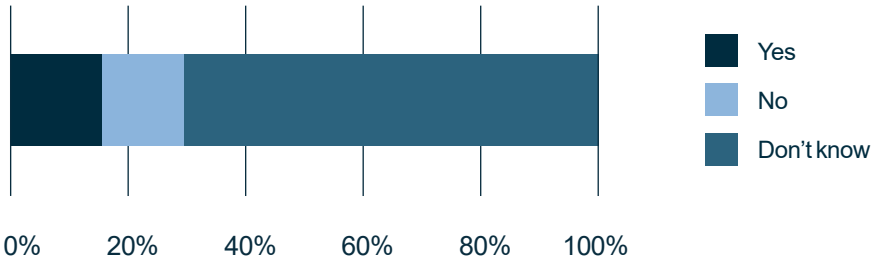
From the free-text responses

Experience of AI as a personnel administration tool.

Does your employer use AI tools to measure or assess your performance?



Does your employer use AI tools to process and/or analyse recordings relating to your work?



More stress when AI is used to assess performance

There is also a clear correlation with stress when employers use AI to measure or assess performance. Among those who state that their employer uses AI, 66 per cent experience greater stress at the same time. The corresponding figure is only 12 per cent among those who state that their employer does not use AI to measure or assess performance. However, the results should be interpreted with some caution, since most respondents answer that they do not know whether their employer uses AI and are therefore not included in this comparison.

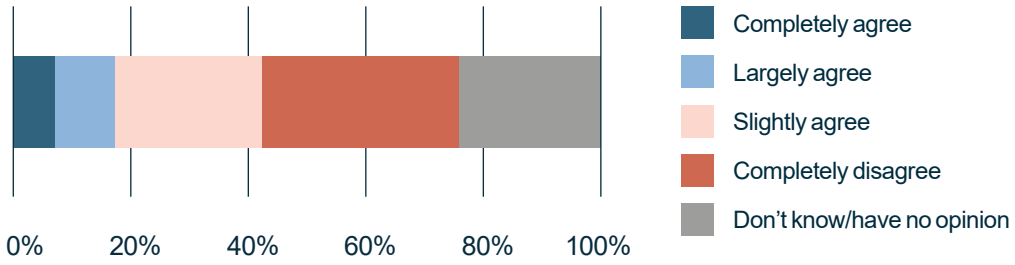


View of the employer

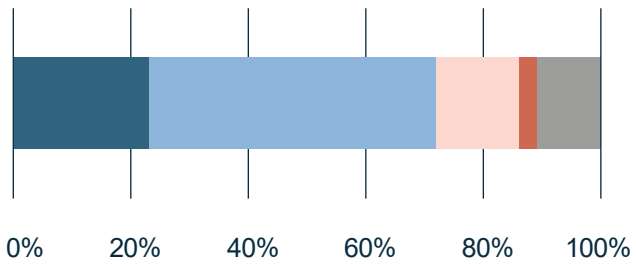
Most state that their employer respects their personal privacy. 72 per cent consider that their employer respects their personal privacy, whereas 17 per cent consider that their employer does not. A small proportion considers the monitoring to be excessive. 17 per cent also consider that their employer monitors their work too much, whereas 58 per cent do not.

"My employer respects my personal privacy" and "My employer monitors too much".

My employer monitors employees too much



Overall, my employer respects my personal privacy



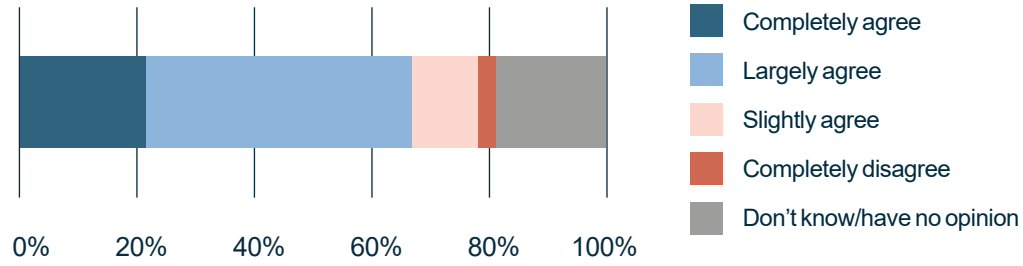
The responses vary according to age and trust is slightly lower, though still relatively high, in the youngest age group: 62 per cent in the youngest group (34 or below) consider that their employer respects their personal privacy, whereas 24 per cent consider that their employer does not. In the remaining age groups, between 72 and 76 per cent state that their employer respects their personal privacy, which is close to the overall average.

There are also some differences when it comes to professional roles and companies. In customer services, 32 per cent state that their employer does not respect their privacy and 36 per cent consider that their employer monitors employees too much. This is also the group that is most subjected to monitoring. However, even within this group, the majority consider that the employer respects their personal privacy. Trust is higher among employees in savings banks: 91 per cent consider that their employer respects their personal privacy.

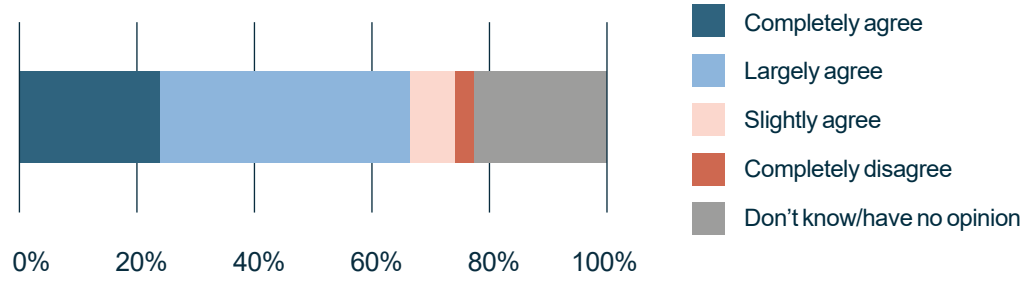
At the same time, 65 per cent consider that their employer has sufficient insight into their work and 66 per cent think that their employer does enough to prevent crime and infiltration. Among those who disagree with these statements, the majority answer that they have no opinion. Only 12 per cent consider that their employer does too little to prevent infiltration or crime and 16 per cent consider that their employer has too little insight into employees' work.

"My employer has sufficient insight" and "My employer adopts sufficient measures against crime"

My employer has sufficient insight into employees' work



My employer adopts sufficient measures to prevent crime, infiltration and other irregularities in activities



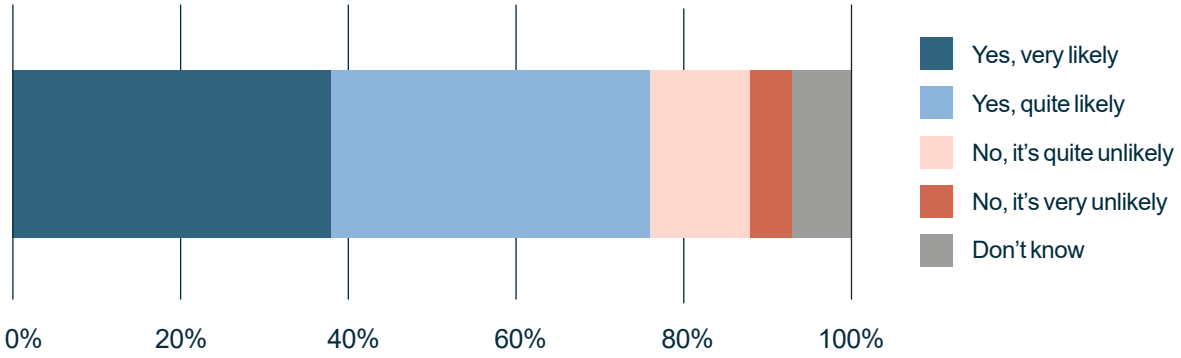
Among employees working in compliance, there are slightly fewer who think that their employer is doing enough to prevent crime, but there is still a majority of 57 per cent who consider that this is the case.

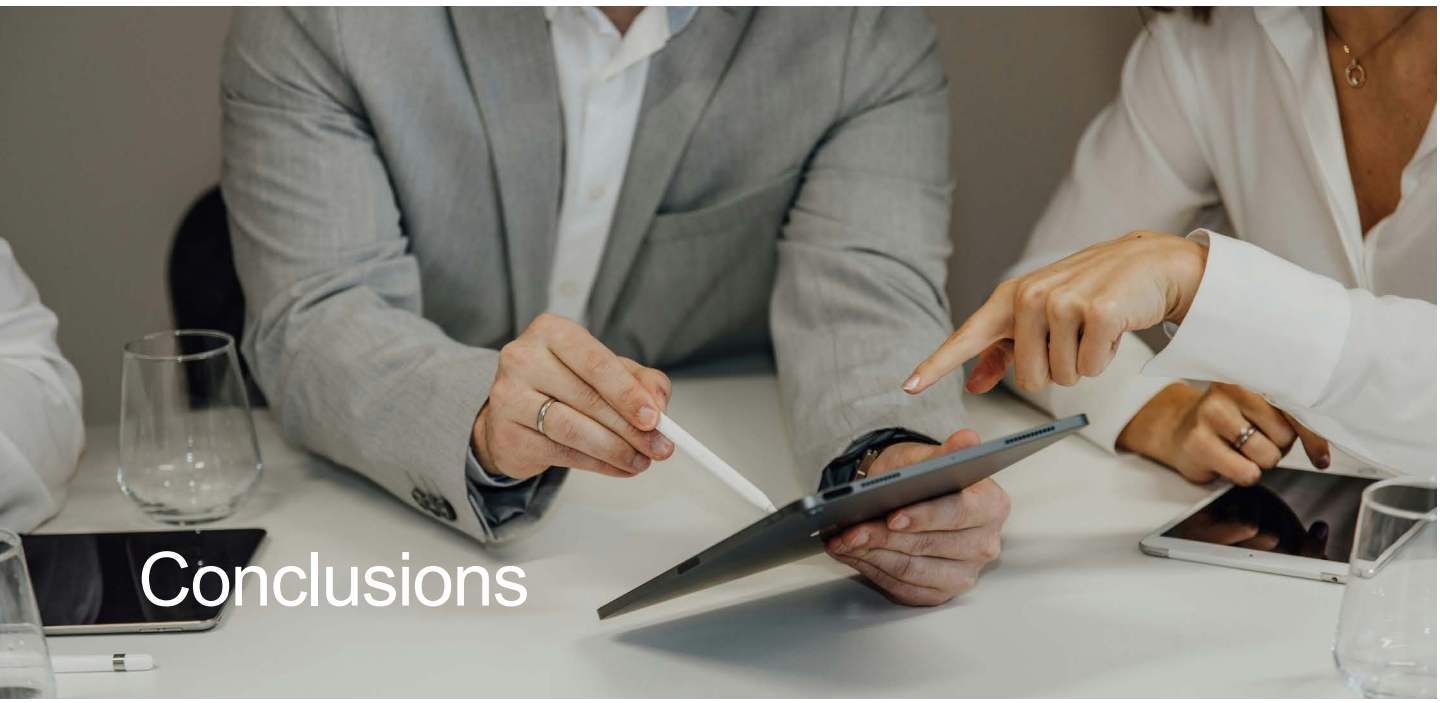
76 per cent of employees would consider changing jobs if they felt that their employer was monitoring them too much.

We have also carried out a comparison with the monitoring index on this issue. However, no correlation is identified here. There is therefore no statistically significant correlation between the level of monitoring and willingness to change jobs if monitoring becomes excessive.

This indicates that attitudes towards monitoring are about the same among employees regardless of the extent of the monitoring they currently experience. Those who state that they experience a low level of monitoring are therefore not more tolerant and it is rather the case that the results reflect actual differences in the work environment.

Would you consider changing jobs if you felt that your employer was monitoring you more than you think is reasonable?





Conclusions

The survey responses show that monitoring in the financial sector is relatively widespread. Many employees provide registry extracts when they begin their employment. Digital systems potentially allow the employer considerable insight into day-to-day work. However, drug tests are still relatively uncommon and are carried out mainly at the time of new employment. The overall picture that emerges is one of monitoring at a level that may be felt to be an intrusion into personal privacy and that risks leading to greater stress for employees.

"Employees are measured more and more. We are measured more than is reasonable and that affects job satisfaction."

From the free-text responses

Widespread monitoring

The report shows that several types of monitoring are common in the financial sector. A clear majority are subjected to some form of digital monitoring and most are subjected to a combination of different types of monitoring. On top of this, there are background checks and drug tests which means, overall, that employers collect a relatively large amount of data on employees.

There appears to be slightly more monitoring in the financial sector than in other sectors. According to researchers at Linköping University, if the labour market is considered as a whole, 63 per cent of managers monitor their employees.[16]This can be compared with the fact that 70 per cent of employees in the financial sector themselves state that their digital meetings are recorded. Despite the fact that it relates to a more specific form of monitoring, it therefore occurs more frequently than digital monitoring seems to occur in other parts of the labour market generally.

Monitoring causes stress

The survey responses provide additional support for the assertion that monitoring leads to greater stress. It affects employees in customer services, advisory services and asset management to a greater extent. The free-text answers indicate that the correlation becomes stronger if the monitoring focuses on performance and individual goals. Such monitoring is likely to be more stressful than data collection that is only carried out for security reasons or that is used to enable incidents to be followed up.

”I am so stressed that I regularly cry after work.”

From the free-text responses

A lack of knowledge

Many employees lack knowledge concerning which data their employer collects. Just over one in three employees do not know whether their employer has access to emails or chat logs, and as many as 54 per cent do not know whether their employer records or can see their screen or mouse and key movements. Also when it comes to many other forms of monitoring, many employees do not know whether it occurs.

That in itself is cause for concern. Employees have a right to know how their personal data is used and what information is stored on them. The fact that so many people answer that that they do not know indicates that they do not receive sufficiently clear information about what this actually consists of.

Elected representatives have slightly more knowledge, but even that group contains a relatively large number of people who do not know what monitoring takes place. This could be a sign that many employers do not cooperate sufficiently with the local trade-union organisation when introducing various forms of monitoring.

“I know that monitoring takes place, but exactly what, when, how and by whom is very unclear, which causes a certain amount of unease.”

From the free-text responses

High level of trust, but trust has its limits

The survey responses show that most employees in the financial sector trust their employer to respect their personal privacy and most do not consider monitoring to be excessive at present. At the same time, a large majority state that they would consider changing jobs if their employer monitored them to an unreasonable extent.

Overall, this suggests a certain sensitivity: Employers should be cautious about increasing the amount of monitoring unless it is clearly justified and employees are fully aware of and in agreement with the need for it. This is also in line with research showing that trust in the employer, loyalty and job satisfaction tend to decline if monitoring is felt to be excessive.[17]

"I think that if you employ a person, you should trust them to do their job. If you think you need to monitor them, you shouldn't hire the person at all."

From the free-text responses

Consequences of monitoring for trade-union activities

General monitoring in the workplace can be a problem for trade-union activities. Contact between elected representatives and members often includes sensitive personal data and trade-union membership in itself constitutes sensitive data. Contact between local elected representatives and members often takes place via work emails, Teams or other channels into which the employer can potentially have insight.

The fact that 64 per cent of elected representatives state that their employer accesses their emails, chats and/or other digital work material is therefore not unproblematic. Over a third of elected representatives state that employers record phone calls and digital meetings to a great extent and another third state that it takes place to some extent. In practice, there is a considerable risk that the employer will thus have access to communications between elected representatives and members.

Some banks have systems in which the computers and phones of white-listed people, including elected representatives, are not monitored to the same extent. But that does not solve the problem of situations in which the elected representative has contact with members who are not white-listed. The communication can then be recorded from the member's device.



Recommendations

The following recommendations are mainly aimed at employers. But trade-union representatives can also contribute to the work, by discussing which measures have the highest priority and highlighting any defects to the employer. Politicians need to contribute in order to strengthen statutory protection.

1. Collaborate on privacy issues

Employers and trade-union representatives should hold discussions about privacy issues in the workplace. Although the requirements of the GDPR focus mainly on rights at an individual level, in practice it is not enough simply to inform individual employees. Elected representatives also need to gain an understanding of what data the employer collects and for what purposes.

Ideally, the parties should hold ongoing discussions over a period of time. There is an obligation under the Co-determination Act and in Finansförbundet's collective agreement with Finansarbetsgivarna to negotiate when new systems are introduced. However, if these discussions are only one-off initiatives, they do not lead to a long-term understanding of each other's needs.

The bank's security protection analysis could form a good starting point for these discussions. The security analysis covers a large number of different factors and must specify which posts are to be included in security classification. In addition, any protective security measures that are necessary must be made clear.[18] Much of the monitoring that takes place with reference to security should be linked to this document. At some companies, the document is managed by the work environment committee, but it can also be the subject of collaboration in other contexts.

2. Increase transparency

Employers must ensure that employees know what type of monitoring is taking place, what personal data is being processed and for what purposes. The survey responses show that knowledge levels are currently poor. There needs to be more information on digital monitoring, particularly in terms of what information is collected and how it is used. There may also be reasons for providing the people who process employees' personal data with greater knowledge: The survey does not examine whether HR personnel or managers have sufficient knowledge of whether employees' personal data is processed. However, the fact that these groups possess a great deal of knowledge can form a solid basis for ensuring that other employees also obtain sufficient information.

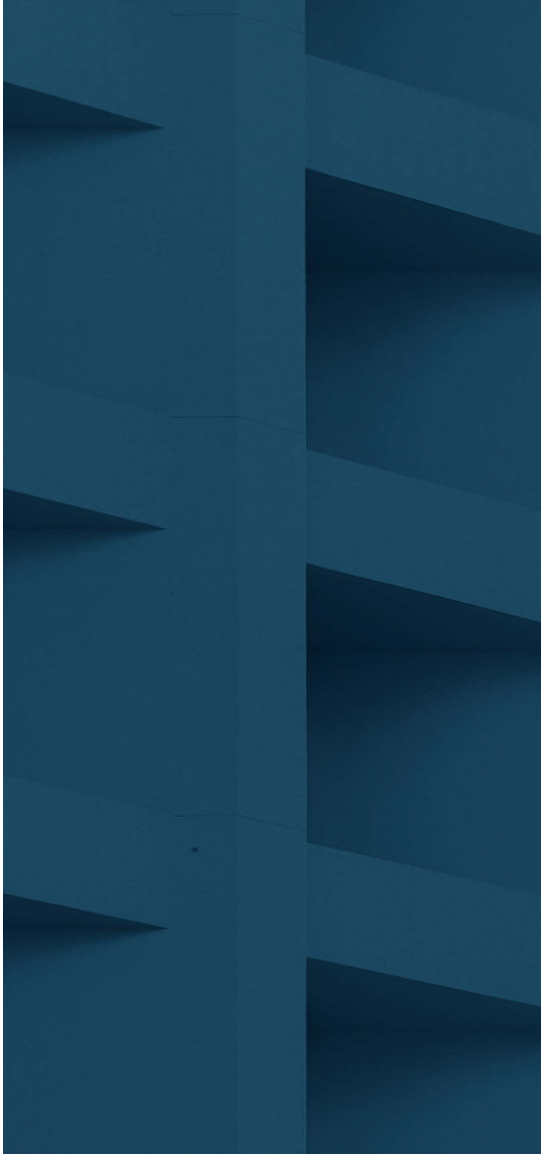
3. Replace, limit, minimise

There is a clear correlation between monitoring, stress and job satisfaction. It should therefore be included in work environment management: Carry out risk and impact analyses when new types of monitoring are introduced. An individual measure may seem harmless, but it is important to also ask oneself how it contributes to the whole. Avoid making monitoring more extensive than is necessary:

- **Replace monitoring with other measures.** There are many other ways to guard against insiders and enablers.[19]

- **Limit monitoring to the right employees.** Customer contacts must often be recorded, which particularly affects employees in customer-related roles, but recording every meeting and phone conversation for every employee in the company is probably not justified.

- **Minimise how monitoring is used.** Monitoring leads to more stress if employees feel that everything they do is being evaluated and measured. The damage can be partially minimised by keeping the number of people who have access to the collected material down, being clear about how the data is used and rapidly weeding out material that has fulfilled its purpose.



4. Promote trade-union privacy

Employers need to ensure that trade-union representatives can have contact with members without being monitored. Systems involving white-listed persons can form part of the solution. If some employees' communications must be recorded, it is also important from a trade-union perspective to clearly define the purpose, clarify that the employer is never permitted to access trade-union discussions, limit who has access to the material and apply the four-eyes principle (duality) in the case of access.

5. Strengthen protection for personal privacy

New legislation is needed in order to further clarify how background checks and registry extracts, drug tests and personality tests may be used. The main protection for employees is currently provided by the General Data Protection Regulation, though the report shows that it is insufficient: Many employees do not know how they are monitored and it can be difficult for many elected representatives to know whether the employer's proportionality assessments are pitched at the right level.

The trade union confederations have previously called for legislation providing comprehensive protection for employees' privacy.[20] The results of this report strengthen the view that such legislation is needed.

Källor

1 OECD, Algorithmic management in the workplace | OECD (2025); ILO, The Algorithmic Management of Work and its Implications in Different Contexts (2022); Eurofound, Employee Monitoring and Surveillance:The Challenges of Digitalisation (2020).

2 EU-kommissionens gemensamma forskningscenter: Electronic Monitoring and Surveillance in the Workplace (2021).

3 Kollega, Bakgrundskontroller har ökat – med 8 000 procent (2026).

4 Sveriges Radio, Fler företag drogtestar personal: ”Bruket finns överallt” (2026).

5 EU-kommissionens gemensamma forskningscenter: Electronic Monitoring and Surveillance in the Workplace (2021) s. 4.

6 Digital transformation stressors in banking: Technostress as a mediator and organizational support as a moderator of job performance - ScienceDirect.

7 EU-kommissionens gemensamma forskningscenter: Electronic Monitoring and Surveillance in the Workplace (2021), ss. 13-19.

8 Europaparlamentets och rådets direktiv 2014/65/EU.

9 Se till exempel Financial Services Union, Employee Experiences of Technological Surveillance in Financial Services (2023) eller Reuters, HSBC plans major global expansion of office, staff surveillance, documents show (2025).

10 Svenska Bankföreningen, Hotbildningsbedömning för Svenska banker 2026 s. 10.

11 The Guardian, Barclays using ’Big Brother’ tactics to spy on staff, says TUC (2020).

12 De rättsliga grunderna beskrivs i dataskyddsförordningens artikel 6, ”Laglig behandling av personuppgifter”.

13 Se vidare Tillåten behandling av personuppgifter i arbetslivet – vilka krav gäller? | IMY.

14 Arbetsdomstolen dom 2024-06-19, AD 2024 nr 46, s. 17.

15 Swedsecs årsberättelse för 2025; Svenska Bankföreningens rapport Bank- och finansstatistik 2025.

16 Kollega, Anställda övervakas – utan att veta om det (2026).

17 EU-kommissionens gemensamma forskningscenter: Electronic Monitoring and Surveillance in the Workplace (2021).

18 Finansinspektionen, Kort om säkerhetsskydd.

19 Se Brottsförebyggande rådet, Möjliggörare för kriminella nätverk (2024) som listar ett flertal andra verktyg: åtkomstskydd; loggning av åtkomst till information; rotering av arbetsuppgifter; fyra-ögon-principen (dualitet); med mera.

20 LO, TCO och Saco, ”Massövervakningen av anställda på jobbet måste regleras”, 2025-05-25

Finansförbundet

is the largest banking and finance trade union in Sweden. We represent everyone working in the financial sector, regardless of educational background or position.

info@finansforbundet.se
Phone: 08-614 03 00
finansforbundet.se

finans förbundet