



# Working with KPMG

**We Do What is Right**

—

# Let's do this

Working with KPMG— v.2

# Introduction



## Our Ethical and Collaborative Culture

---

At KPMG, our ethical and collaborative culture is critical to achieving our trust and growth ambition, and our long-term success as a business.

- ✓ It helps us attract and retain the best people and be the kind of workplace that you want to work in.
- ✓ It provides a foundation for our relationships with our clients, the entities that we audit, regulators, strategic alliance partners and vendors and other stakeholders.
- ✓ It underpins the trust that our clients, our people, our stakeholders, and society at large have in us. This trust is essential if we are to accelerate our growth and capture additional market share.

Our commitment to upholding our Values is clear: there is **never** a situation – either insider or outside of our work at KPMG – where compromising our standards of behavior is acceptable.

Our ethical and collaborative culture grows stronger when we all take personal responsibility for living out Values in everything that we do and we hold each other accountable for doing so.

# Topics

We do what is right: Integrity at KPMG



**Our Values and Global Code of Conduct**



**Ethics checklist**



**Bribery**



**Insider trading**



**Confidential information**



**Competition law do's and don'ts**



**Speak up**

# Our Values: What we believe



## Integrity

We do what is right.



## Excellence

We never stop learning and improving.



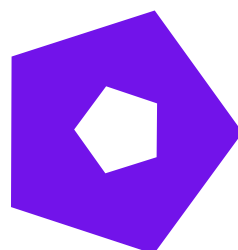
## Courage

We think and act boldly.



## Together

We respect each other and draw strength from our differences.



## For Better

We do what matters.



Click each value to learn more

# Integrity

We do what is right



## What it means

- Consistently leading by example with high standards and morals
- Being honest and truthful in words and actions
- Navigating pressures honestly, in a challenging environment

Integrity means we are honest, fair and **consistent** in our words, actions and decisions – both inside and outside work. We take **responsibility and accountability** for our day-to-day behavior and we hold ourselves to the **highest moral and ethical standards** at all times – even when **under pressure**. We keep our promises and set an example for others to follow.



## Key themes

Honesty, fairness, keeping promises, accountability

# Excellence

We never stop learning and improving



## What it means

- Setting the standard for and executing with quality
- Continuously building on current performance and culture
- Taking responsibility and accountability for actions

Excellence means relentlessly **delivering quality work to the highest professional standards**. We do this by staying **curious and taking personal responsibility for our learning**. We constantly look to improve our work through **data and insight**, and are **open to new challenges and feedback** because that is how we develop and improve.



## Key themes

Quality, professional standards, going beyond, continuous learning

# Courage

We think and act boldly



## What it means

- Communicating openly and directly
- Striving for innovation and new thinking
- Relentlessly pursuing differentiation in the market

Courage is about being **open to new ideas** and **being honest** about the limits of our own knowledge and experience. It's about **applying professional skepticism** to what we see and **asking questions where we have doubts**. We **speak up** if we see something we believe is wrong and we **support those who have the courage to speak up themselves**. Courage is being **bold enough** to step outside of your comfort zone.



## Key themes

Speak up, feedback, innovation, confidence

# Together

We respect each other and draw strength from our differences



## What it means

- Showing care and consideration for others
- Embracing diversity and acting inclusively
- Collaborating within and across teams

We do our **best work when we do it together**: in teams, across teams, and by working with others outside our organization. Working together is important because we know it's **collaboration that shapes opinions** and drives creativity. We embrace people with **diverse** backgrounds, skills, perspectives and life experiences and ensure different voices are heard. We show **care and consideration** for others and strive to create an **inclusive environment** where everyone feels they belong.



## Key themes

Collaboration, inclusion, care, belonging

# For Better

We do what matters



## What it means

- Serving and strengthening our markets and communities
- Making the firm better for future generations
- Making a positive impact on society

For better means taking a **long-term view**, even in our day-to-day choices, because we want to build a **stronger KPMG for future**. We never lose sight of the importance of our role in **building trust** in the capital markets and in business. We make **sustainable, positive change** in our local communities and in society at large, **striving to make the world a better place**.



## Key themes

Long-term view, stewardship, society, purpose

# Code of Conduct

**The Global Code of Conduct (the Code) guides our actions both inside and outside of KPMG. It includes:**

**Our Values**

**Our  
Commitments**

**Our  
Responsibilities**

**Where  
to get help**

**Compliance  
with the Code  
of Conduct**

The Code expressly sets out the ethical behaviors expected of everyone at KPMG. It defines what it means to work at and be part of KPMG, as well as our individual and collective responsibilities.



The Code is available via [link](#)

# Ethics checklist

The Ethics Checklist is a resource within the Code to help you when you're faced with difficult decisions or situations, as well as when you're going about your daily business at KPMG.

It includes questions such as:



Is my behavior consistent with KPMG Values and ethical or professional standards?



Does my decision reflect the right thing to do?



Does my action comply with KPMG policy and applicable laws or regulations?



Am I confident that my decision would not cause KPMG reputational and brand damage if it were made public?

Thinking about these and other questions in the Ethics Checklist can help increase your awareness of the factors that subconsciously influence decision-making and which could lead you or someone else at KPMG to act in a way that is contrary to our Values.

# Bribery

KPMG has zero tolerance for bribery and corruption in any form by anyone at KPMG and by those we may have dealings with. We are committed to conducting business fairly and ethically, and avoiding even the perception that KPMG or its people would offer or accept a bribe to obtain an advantage.

Be careful that offering or receiving gifts and entertainment doesn't cast doubt on KPMG's or your own integrity, independence, objectivity or judgment.



# Insider trading

When you work at KPMG, irrespective of your role, you may become aware of non-public information that relates to a relevant company or its securities; this is called inside information.

Engaging in insider trading is against KPMG policy. Many countries have specific laws prohibiting insider trading, and other countries may have more general criminal and/or civil laws that are used to penalize this type of behavior.

Any KPMG person found to have violated our insider trading policy is likely to be subject to serious disciplinary action up to and including termination of partnership/employment. Any KPMG person in violation of insider trading laws may also be subject to criminal prosecution.



# Confidential information

**Most of the information that KPMG creates, collects and shares is sensitive in some way and everyone has an essential part to play when it comes to protecting it.**

Under no circumstances should you use it to your own advantage or the advantage of others, disclose it outside of KPMG or share it with someone internally who doesn't have a business need to know it.

Many jurisdictions have specific laws and regulations on confidentiality as well as data privacy. Know and comply with the laws and regulations that apply to you and the work that you do.

If you believe that confidential information and/or equipment used to store such information has been lost, stolen or otherwise compromised, immediately report the matter following KPMG firm's procedures.



# Protecting confidential information

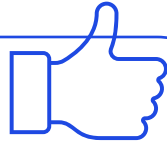
**No matter where you work – at home, at your KPMG office or workspace, or at a client location — here are some tips to keep confidential information and your KPMG technology resources safe and secure.**

- ✓ Lock or secure portable devices, including laptops, phones and USB drives at all times – including when you are traveling.
- ✓ Use a laptop security screen and lock your laptop screen when leaving your desk temporarily.
- ✓ Never share your password or other credentials with anyone.
- ✓ Collect and use only the information you need. Return or properly dispose of it as soon as it's not needed (subject to our retention policies).
- ✓ Never leave confidential papers, etc. unattended on your desk, at a printer or anywhere else.
- ✓ Use only KPMG-approved, secure and encrypted storage devices and KPMG-approved software and apps.
- ✓ When sending emails, especially group emails, ask yourself: “Do they all really need to know this?”
- ✓ Be careful and select the correct persons when adding addressees to an email.
- ✓ Think before opening attachments or clicking on links in emails.
- ✓ Take care with conversations in public places, at home and when traveling.
- ✓ Use a meeting room or other private space when having a confidential conversation by phone, Skype, Microsoft Teams, or other electronic method.

# Competition law do's and don'ts

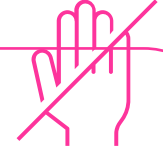
**Take care in your conversations with KPMG competitors so that you don't violate competition law and KPMG policy:**

## DO



- Limit any discussions to formal meetings set up for that purpose, set an agenda and document meeting minutes. Breaches are more likely to occur in informal or social settings.
- Get legal counsel to attend any meeting that you think may deal with particularly sensitive issues.
- Immediately raise any concerns you have during a meeting about the appropriateness of any topic under discussion – the discussion should not continue until your concerns have been resolved. If this is not possible, consider leaving the meeting and ensure that your departure is recorded. There may also be a reporting obligation here even if you've only been the recipient of commercially sensitive information. Report the matter to RMP or legal department.

## DON'T



- Disclose (or encourage or allow competitors to disclose to you) any commercially sensitive information, in particular, any strategic information that could give insight into KPMG's current or future competitive actions.
- Make statements or divulge information which you would feel uncomfortable reading on the front page of the following day's newspaper.
- Agree with competitors to share customers, markets or territories; to fix prices or other terms of engagement with customers; to refrain from bidding for a customer contract or to do so at a particular price; or to take action with a view to excluding them from particular markets, territories or customers.
- Take on any joint research or analysis with a competitor without first seeking advice from appropriately qualified legal counsel on how to set up appropriate safeguards to protect any inappropriate disclosure of information.

# Speak up

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.



**Engagement partner**



**Ethics and independence partner (EIP)**



**Risk management partner (RMP)**



**Other reporting channels**



**KPMG International hotline**

**KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.**

Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. **The important thing is that you speak up!**

# Speak up

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.



Engagement  
partner

Contact your engagement partner for matters that relate to his or her clients, including (1) non-compliance with laws or regulations by clients or third parties, and (2) breaches of KPMG policy or non-compliance with laws, regulations or professional standards by KPMG firms or personnel.

Ethics and independence  
partner (EIP)

Risk management  
partner (RMP)

Other reporting  
channels



KPMG International  
hotline

**KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.**

Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. **The important thing is that you speak up!**

# Speak up

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.



Engagement  
partner



Ethics and independence  
partner (EIP)

Contact EIP in the case of breaches relating to ethics and independence matters by KPMG firms or personnel. Independence breaches should be reported immediately!

Risk management  
partner (RMP)

Other reporting  
channels

KPMG International  
hotline

**KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.**

Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. **The important thing is that you speak up!**

# Speak up

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.



**Engagement  
partner**



**Ethics and independence  
partner (EIP)**



**Risk management  
partner (RMP)**

Contact RMP on matters not involving clients (as you would usually report client-related matters to the engagement partner). If you believe the engagement partner is in some way involved in the matter or is not dealing with an issue in the appropriate way, escalate the matter to your RMP!

**KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.**

Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. **The important thing is that you speak up!**

# Speak up

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.

These include your supervisor, line manager, or performance manager, your KPMG firm's human resources team or its internal legal counsel. Your KPMG firm may also have a confidential reporting mechanism such as a "whistle-blowing" hotline or an ombudsman.

Local laws or regulations, such as anti-money-laundering reporting legislation, may require you to report in a certain way or to a particular person.

There are also individuals from outside your own KPMG firm to consider contacting. These include Global Quality & Risk Management, International Office of General Counsel, and regional risk management partner.



**Other reporting  
channels**



**KPMG International  
hotline**

**KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.**

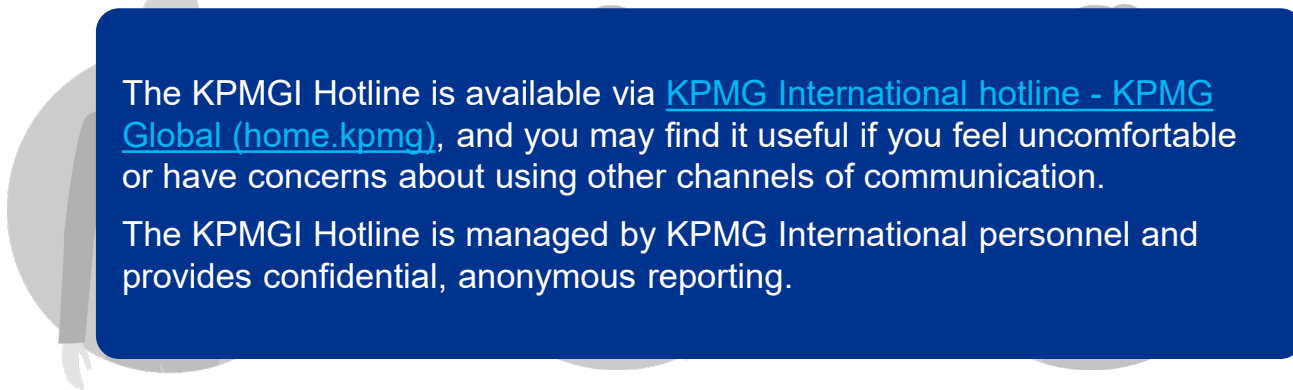
Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. **The important thing is that you speak up!**

# Speak up

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.



Engagement  
partner



Ethics and independence  
partner (EIP)

Risk management  
partner (RMP)

Other reporting  
channels



KPMG International  
hotline

**KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.**

Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. **The important thing is that you speak up!**

# Speak up

Using KPMGI Hotline facilitates confidential reporting of possible illegal, unethical, or improper conduct at the firm relating to accounting, internal accounting controls, auditing, banking crime, financial crime, anti-bribery or workplace harassment when the normal channels of communication have proven ineffective, or are impractical under the circumstances.



## Concerns can be reported in two ways:

- By accessing a web-based reporting system at: [www.clearviewconnects.com](http://www.clearviewconnects.com) (use KPMG International)
- Via mail: ClearView Connects P.O. Box 11017 Toronto, Ontario M1E 1N0, Canada

The Hotline is designed to protect your confidentiality, and your anonymity, if requested.



# Independence Training

# Welcome to KPMG

KPMG is a regulated business which means there are lots of rules, regulations and laws which the firm and you must comply with. These slides provide you with an overview of what's important for you to know before you start working with KPMG.

## In particular you will learn about:

Your responsibility and the commitment required to meet the highest principles of ethics and integrity through personal behaviours that are consistent with KPMG's Code of Conduct



How regulation affects the business we work in and how this impacts you personally

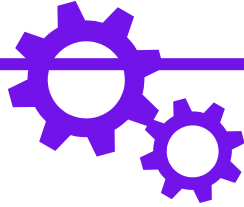


The channels available to you if you need advice or have to report a concern.



# Working in a regulated environment

01



Working in a regulated environment means our work is under constant scrutiny. Regulators act in the public interest to ensure high standards of professional work by our firm and firms like us. As a result we are constantly in a bright spotlight, with our work under a magnifying glass that is growing larger and larger

02



Working in a regulated environment means there are strict rules about our work, what we can and can't do and with whom we can and can't work. Standards are very high and failure to comply with these rules is not an option. There is no margin for error. Consequences are immediate and can be severe

03



The rules exist for a reason – they are put in place to protect those who use our services and rely on our work to be accurate, objective, and truthful

# Insider trading

You are prohibited by law (as well as by KPMG policies) from insider trading. Working at KPMG will result in your being privy to inside information which you must never use (either yourself directly or to assist others).

Penalties for insider trading can be severe – including substantial fines, lengthy prison sentences and the confiscation of gains. For everyone involved, the financial, legal and reputational damage caused is significant.

If inside information is leaked to the media or other external sources, there could additionally be significant financial and reputational impact on the client as well as on KPMG.

Inside information that you obtain during the course of a client engagement or whilst working with KPMG is confidential information; both KPMG and the client may take additional legal action if you are involved in any breach in confidentiality.

**Anyone who violates KPMG's policy on insider trading is likely to have their contract terminated without notice and face criminal charges.**

**Insider trading:** The buying or selling of a security or investment (for example, stocks, shares, bonds, derivatives, etc.) while in possession of inside information.

Inside information is specific non-public information which relates to a relevant company or its securities. Typically information will be 'inside information' if, when made public, it may have a significant impact on the price of the securities or investment and/or is information which a reasonable investor would consider significant in deciding whether to buy, hold or sell the securities or investments.

**Confidential Information:** Any information that comes to an individual's attention as a result of the individual's association with KPMG, unless such information is publicly available.

In addition to inside information, this includes any information obtained in the course of your work and includes KPMG knowledge, methodologies, and other such material, as well as information about former or current clients and other third parties.

# Gifts & Entertainment

A member of the audit team shall not accept gifts or hospitality from a restricted entity unless the value is trivial and inconsequential.

KPMG policies also prohibit any KPMG personnel from accepting gifts or entertainment where the monetary value, duration or nature is such that it may cast doubt on the integrity, independence, objectivity or judgment of KPMG or the individual (or constitutes a bribe or would otherwise breach applicable laws).



# Why do the independence rules exist?

Firms like KPMG are regulated – which means there are specific standards we must meet while going about our work. Regulators exist to set standards and crucially to protect clients and the public.

Part of KPMG's business is to audit the financial statements of other businesses. Users of these financial statements want to know whether they can be relied on –and that's where our audit provides value. But to do this, **we have to give an unbiased and professional opinion – to be objective** –and that means we (i.e. KPMG and everyone who works for KPMG) have **to be independent**.

## The challenge

Independence-related matters continue to make headlines throughout the world. The independence of audit firms (including KPMG) has been called into question.



Following the economic crisis and subsequent economic recession, our regulators have worked tirelessly to develop and enhance the rules and regulations we must follow – all as a means for providing the public with confidence that firms like KPMG can provide an independent audit opinion.

# Independence matters for contractors too!

As a contractor engaged by KPMG for a specific period of time or for a specific project you will generally not take on an engagement leader or engagement manager role. If your contract is to assume an engagement leader or managerial role, please advise the KPMG Ethics and Independence team, Risk management department as you will need to complete a different training module for your role.

As you will generally not be in the engagement leader or managerial role, most of the work that needs to be undertaken to confirm and monitor our independence will be completed by a KPMG partner or employee.

## HOWEVER, you do need to know the basics for 2 key reasons:

You may need, even though you are not a KPMG employee and perhaps not working directly in the audit function, to comply with the personal independence rules

You need a very basic awareness of how independence affects the work we do so you can understand the larger picture of how relationships with our clients fit together across all of KPMG's service offerings

You are required to be independent even though you aren't a KPMG employee if your work is for a KPMG audit client.

If you are asked to take on the role of engagement leader, speak up! KPMG policies prohibit contractors from taking on such a role without Risk Management knowledge. Please contact Risk management department.

# There are consequences for everyone

There are consequences if you, your colleagues or the firm don't comply with the independence rules (and KPMG's policies that make the rules real for our firm).

## These include:

### For you personally

- You may be removed from the KPMG engagement and your employment contract may be terminated by your firm
- You may be subject to disciplinary action by any professional body of which you are a member
- You may lose work from other clients who see compliance by their auditors/advisors with independence rules and regulations as vital
- You may be given a personal fine by the regulators
- You may have to dispose of investments — possibly at a loss

### For KPMG

- The firm's reputation can be damaged
- The firm may be investigated by the regulators
- Fines can be imposed by the regulators
- Client(s) may choose to end their working relationship with KPMG
- KPMG may lose other/future work from existing and potential clients

**The impact of getting it wrong is severe which is why KPMG has a zero tolerance policy for failure.**

**Your valuable reputation is at stake along with KPMG's and your firm's, so please take responsibility for helping us to get independence right**

# Personal independence

The independence rules apply to us personally because our regulators, the public, our clients and the profession want to avoid any personal circumstances affecting, or being perceived to affect, the work that KPMG does.

## Things you need to be aware of:

If you are providing any services on KPMG's behalf to an audit or assurance client, you are prohibited from holding shares or financial interests in that client. This rule also applies to your immediate family members

If any of your immediate or close family members work for an audit or assurance client and you are asked to work on an engagement for that client, please notify the Engagement Partner prior to beginning any service

If you are asked to work on an audit client which is itself or part of a group registered on the Securities and Exchange Commission (SEC) in the USA, the personal independence rules are more restrictive. If you are asked to work on such a client you must complete the **Independence Declaration** for SEC Issuer Audit Engagements and discuss with the Engagement Partner any potential independence issues prior to commencing work

If you are working on a Financial Services audit or assurance client, the rules are more complicated, so please consult with the Engagement Partner

The rules are complex and while you are not expected to be an expert on all regulatory matters you do need to be aware of and comply with our 'personal independence' policies.

### Immediate family

spouse (which includes your spouse equivalent whether or not you are married), and dependents (children and others, for example, dependent parents)

### Close family

siblings, parents, and non-dependent children

# Outside activities and other relationships

01

Activities and relationships we have outside KPMG can also impair our independence



02

Activities such as acting as a company director or employee of any KPMG audit client will result in a breach of our independence requirements



03

**You must therefore disclose ALL outside activities** (positions in the last 12 months, current or in the future) **to KPMG Risk Management before starting / continuing work with KPMG**



# Covered Persons and Restricted Entities

## The “Covered Person” concept is important in determining your independence — but what does it mean?

Some people believe that the concept of covered persons is limited solely to audit partners and audit staff. But this is incorrect. The fact is, you may be a covered person even if you do not provide audit services. A covered person is any KPMG professional who has any of the following relationships with a restricted entity.

### Audit Services



#### Members of the audit team, including:

- All partners and professionals participating in the audit engagement.
- All individuals in the **chain of command**.

#### Applies to:

All partners and professionals including contractors, and their **immediate family** members

### Non-Audit Services

Partners and managerial employees or contractors in a managerial position who provide 10 or more hours of non-audit services to the audit client

#### Applies to:

Partners and professionals including contractors (manager and above), and their immediate family members




### ‘Office’ Relationships



All partners located in the **office** where the **lead audit engagement partner** primarily practices in connection with the audit engagement.

#### Applies to:

Partners only and their immediate family members



**Note:** For purposes of the restrictions on investments, the definition of “Covered Person” is extended to include any other professional (including contractors) providing, or expecting to provide, 10 or more hours of non-audit services to the client. Refer to the guidance “Personal Interests – Independence Policies on Investments” for more information.

#### Restricted Entities include:

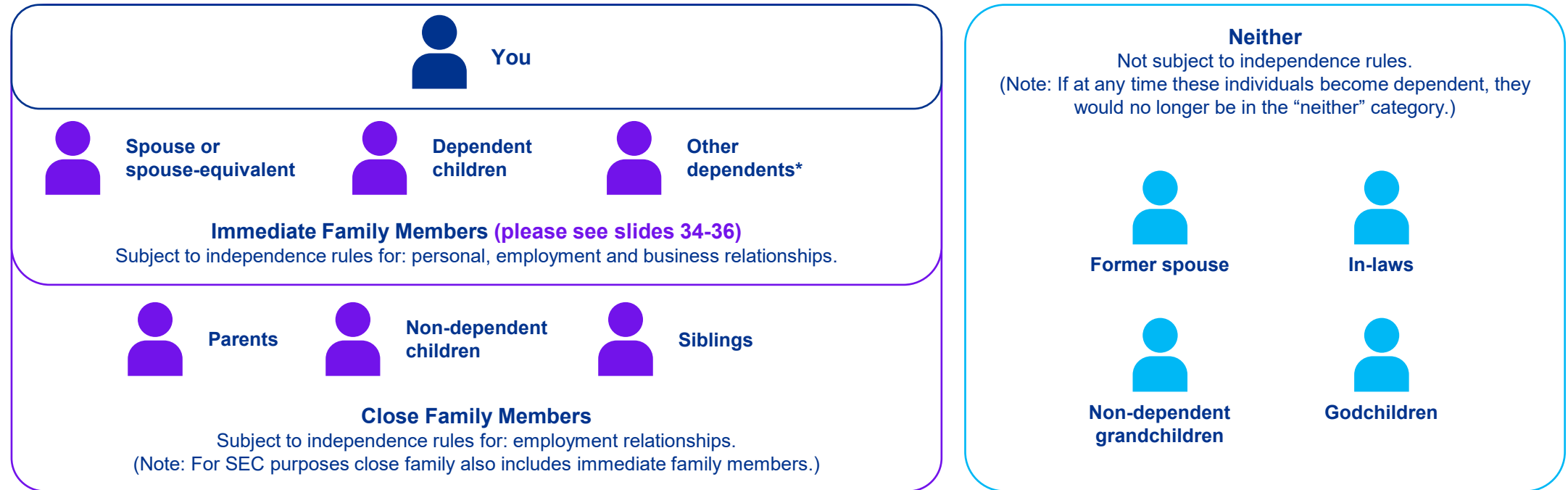
- An audit or assurance client
- ‘Affiliates’ of an SEC audit client
- ‘Related entities’ of an audit or assurance client in accordance with the International Code of Ethics for Professional Accountants



# Independence and Your Family

The independence rules apply to you and to certain members of your family.

The diagrams here illustrate which family members are affected by KPMG independence policies:



\*Receive more than half of their support from you or your spouse / spouse equivalent or both in most recent calendar year.

# Family Employment Relationships

It is unavoidable that family members of professionals will work for restricted entities. Not all employment will cause an independence issue; it will depend on the professional relationship to the audit client, the proximity of the family relationship, and the nature of the family member's employment.

Situations in which an **immediate family member** has influence over our client's financial reporting can create a threat to our independence. In these situations, the professional must be removed from the audit team. If the relationship is one of a **close family member**, it may be possible to deal with it by applying appropriate safeguards.

**International Code of Ethics for Professional Accountants** prohibits all situations in which an immediate or close family member of the audit team member has an accounting or a financial reporting oversight role at the audit client.

## SEC Restricted Entities

The SEC prohibits all situations in which a close family member of a covered person fills an accounting or financial reporting oversight role



## Glossary

### Immediate family member

a spouse (or equivalent), dependent children or other dependents. A dependent is any individual who received more than half of his or her support for the most recent calendar year from the relevant individual (e.g. the KPMG member firm professional, his or her spouse (or equivalent) or both). A dependent may be an unrelated person

### Close family member

includes parents, non-dependent children and siblings. For SEC purposes the definition of 'close family member' also includes 'immediate family members'

### Restricted Entities include:

- An audit or assurance client
- 'Affiliates' of an SEC audit client
- 'Related entities' of an audit or assurance client in accordance with the International Code of Ethics for Professional Accountants



# Family Employment Relationships

## IESBA Code Restricted Entities

### Who is affected?

Members of the audit team



### What is our policy?

When a member of the audit team has a family member in the following positions there is a threat to independence:

- Director
- Officer
- A professional in a position to exert significant influence over the preparation of the client's accounting records or financial statements on which the performing member firm will express an opinion

If the person in one of the above positions is an immediate family member, the professional must be removed from the audit team.

If the person in one of the above positions is a close family member, the audit team member shall, promptly on identification of such relationship, consult the Lead Audit Engagement Partner or their KPMG member firm Ethics and Independence Partner (EIP). However, where the audit client is a Reporting Issuer, such situations cannot be safeguarded.

When an immediate family member of a member of the audit team is an employee of the audit client in a position to exert significant influence over the client's financial position, financial performance or cashflows, you must promptly consult with the Lead Audit Engagement Partner or Ethics and Independence Partner.

### Audit Team

(a) All members of the engagement team for the audit engagement

(b) All others within the KPMG member firm who can directly influence the outcome of the audit engagement, including those who:

- recommend the compensation of, or who provide direct supervisory, management or other oversight of the LAEP in connection with the performance of the audit engagement. This includes those at all successively senior levels above the LAEP through the member firm's chief executive/senior partner
- provide consultation regarding technical or industry specific issues, transactions or events for the audit engagement
- provide quality control for the audit engagement (including where applicable the EQCR Reviewer)

(c) All those within another member firm who can directly influence the outcome of the audit engagement

(a) and (b) together are referred to as the "chain of command". The chain of command will not extend beyond a KPMG member firm to KPMG International or any of its officers or employees

# Family Employment Relationships

## SEC Restricted Entities

### Who is affected?

Covered persons. Refer to the guidance "Covered Persons" for more information on who is considered a covered person

### What is our policy?

Close family members of covered persons may not be **in an accounting or financial reporting oversight role** with a restricted entity

### What if the close family member does not have one of the listed titles / positions?

Some people may perform an accounting or financial reporting oversight role, even though their title does not reflect it. For example, a "project coordinator" with responsibility to test and document financial reporting controls under Sarbanes Oxley Section 404, a position comparable to Director of Internal Controls Compliance, is in a position to exert influence over financial reporting.

Therefore, it is important to assess the substance of the family member's role with the restricted entity, not just his or her title. In making decisions about whether someone, without the title, is in a financial reporting oversight role, you are encouraged to consult with the Engagement Partner.

### Accounting role

A role in which an individual is in a position to or does exercise more than minimal influence over the contents of the accounting records, or anyone who prepares them.

Individuals having primary responsibility for accounting functions that support material components of the financial statements are considered to be functioning in an accounting role

### Some Titles/Positions Generally Deemed to be Financial Reporting Oversight Roles

- |   |   |
|---|---|
| — Members of the Board of Directors (or similar management or governing bodies) | — Controller  |
| — Chief Executive Officer   | — Director of Internal Audit  |
| — President   | — Director of Financial Reporting   |
| — Chief Financial Officer   | — Treasurer   |
| — Chief Operating Officer   | — Director of Internal Controls Compliance (or similar management positions responsible for compliance under Section 404 of the Sarbanes-Oxley Act of 2002) |
| — General Counsel   |   |
| — Chief Accounting Officer  |   |

### Financial Reporting Oversight Role

A role in which an individual is in a position to or does exercise influence over the contents of the financial statements, or anyone who prepares them.

#### Examples:

CEO, President, CFO, COD, General Counsel, Controller, Director of Internal Audit, and Director of Financial Reporting

# Independence Policies on Investments

Your personal independence may be affected if you, or an immediate family member, has or is thinking about making an investment, obtaining a loan or entering into other financial relationships.

This document explores KPMG's policies on making investments.

Investments (also referred to as “financial interests”) include stocks, bonds, options, mutual funds, and other securities.

Prior to starting any services for an audit client, you need to check whether you have any investments in the audit client or their affiliates (restricted entities).

If you have any investments in a restricted entry, speak to the Engagement Partner before commencing any service to determine potential independence issues.



## Restricted Entities include:

- An audit or assurance client
- ‘Affiliates’ of an SEC audit client
- ‘Related entities’ of an audit or assurance client in accordance with the International Code of Ethics for Professional Accountants



# Independence Policies on Investments

## Who is affected?

Covered persons and **other restricted professionals** and their immediate family members. Refer to the guidance "Covered Persons" for more information on who is considered a covered person.

Any other professional including contractors providing, or expecting to provide, 10 or more hours of non-audit services to the client

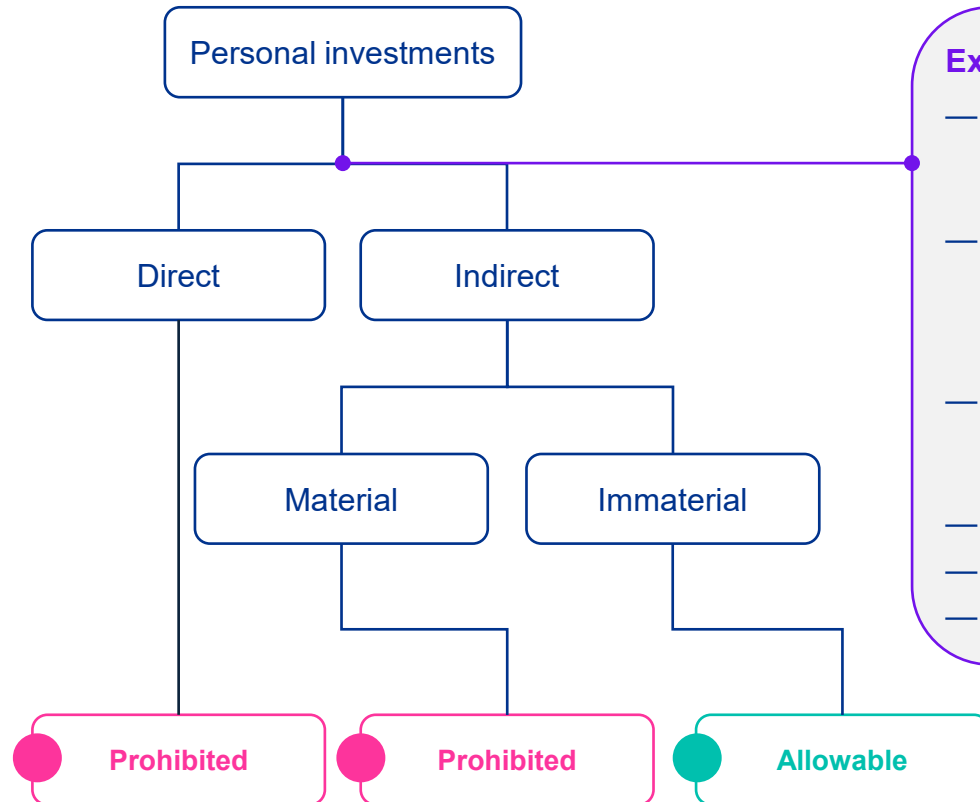


## What is our policy?

You may not hold, or be committed to acquire, any direct or material indirect financial interests in a restricted entity. Before entering into a financial relationship with any entity, you must fully investigate to ensure that the entity is not restricted.

Additional guidance is provided on upcoming slides on "Personal Interests: Independence Policies on Other Financial Relationships" to read about the exception for Spouse and Dependent Benefit Plans.

# Independence Policies on Investments



## Examples of Investments (Financial Interests):

- Stock or other securities or rights to acquire such securities, and rights of participation, as well as options or warrants to acquire an interest, and other vested rights and other derivatives
- Other securities such as bonds, i.e. a debt security, in which the authorized issuer owes the holders a debt and is obliged to pay interest and/or to repay the holder at a later date; a bond can be issued by a private entity, the state or local government, etc.
- Financial arrangements with investment companies where the investor is eligible and/or able to receive a distribution of securities (e.g. Unit Investment Trust (in US))
- Investments in mutual funds or exchange traded funds
- Participation in investment clubs or trusts (including blind trusts)
- An interest in a partnership

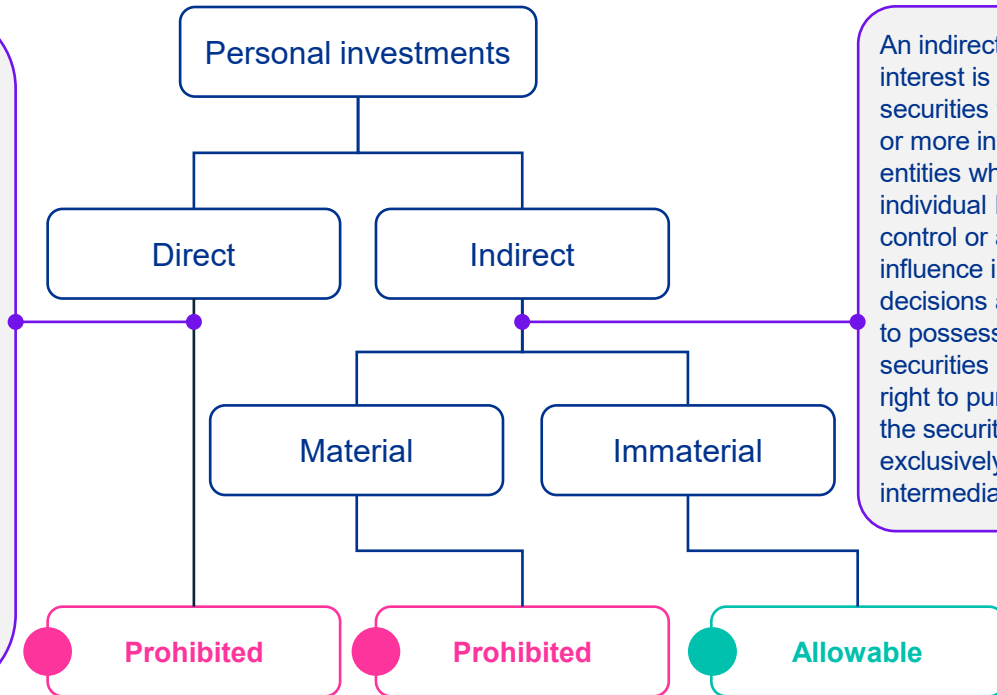
# Independence Policies on Investments

A direct financial interest is just as the name implies; it is an investment in an entity. A direct investment in a restricted entity, no matter how small or how long ago you purchased it, impairs your independence.

It also includes financial interests owned or controlled directly by an individual or entity (including those managed on a discretionary basis by others).

## Direct financial interests include:

- Investments in mutual funds (these are direct financial interests in the fund itself.)
- Investments entered into as a result of membership in an investment club.
- Investments in investment vehicles which you have set up, or which have been set up to your benefit (e.g. trust.)
- Financial interests beneficially owned through an investment vehicle, estate, trust, or other intermediary when the beneficiary controls the intermediary or has the authority to supervise or participate in the investment decisions.
- An interest in a partnership where the individual is a general partner.
- Investment in a limited partnership or similar entity (these are direct financial interests in the limited partnership itself, but not necessarily in investments made by the limited partnership.)



An indirect financial interest is ownership of securities through one or more intermediary entities where the individual has no control or ability to influence investment decisions and the right to possess the securities (including the right to purchase or sell the securities) rests exclusively with the intermediary entities.

## SEC Restricted Entities

In addition to the above, the SEC also considers the following investments to be direct financial interests:

- Interests in restricted entities through an intermediary if the KPMG member firm, covered person, or immediate family member, alone or together with other persons, supervises or participates in the intermediary's investment decisions or has control over the intermediary.
- Ownership through a non-diversified mutual fund that has an investment in a restricted entity which amounts to 20% or more of the value of the mutual fund's total investments. (If a fund is non-diversified, this fact must be disclosed in its prospectus).

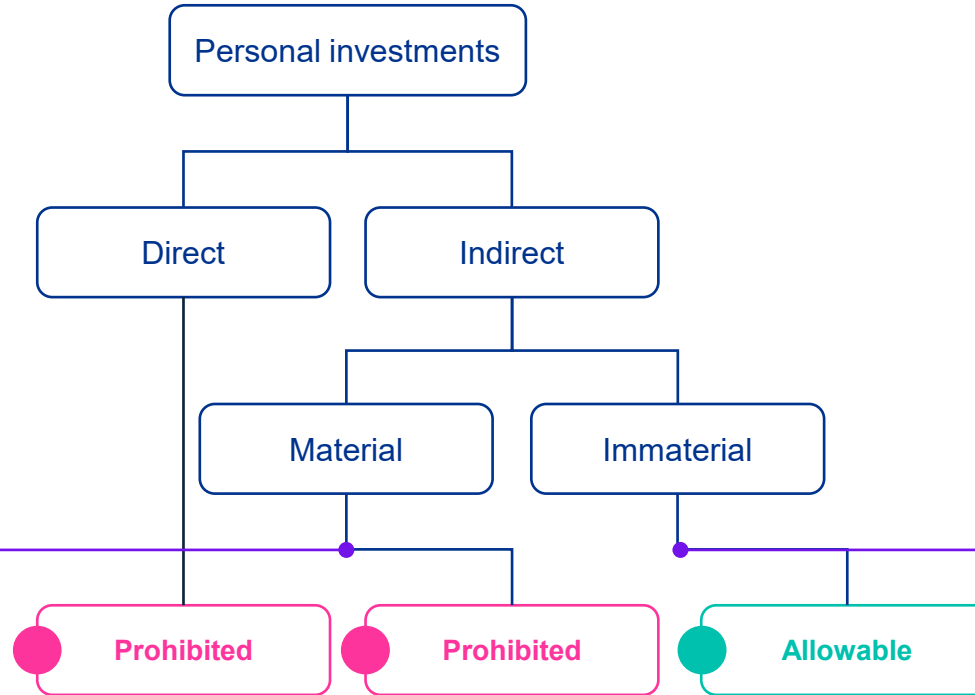


# Independence Policies on Investments

## Material

The investment is equal to 5 percent or more of the individual's net worth (the combined net worth of the individual and the individual's immediate family members may be taken into account).

To calculate your own net worth, you add the value of the assets you own (including but not limited to cash, securities, personal property, real estate, and retirement accounts) and subtract your liabilities (or what you owe in loans and other obligations).



## Immaterial

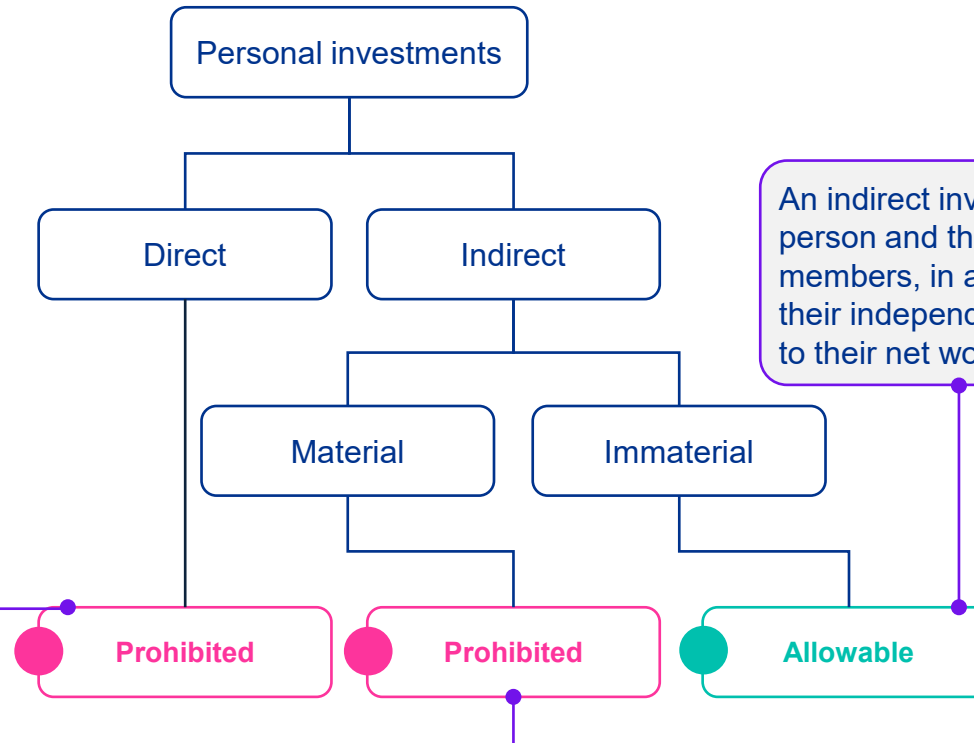
The investment is less than 5 percent of the individual's net worth (the combined net worth of the individual and the individual's immediate family members may be taken into account).

To calculate your own net worth, you add the value of the assets you own (including but not limited to cash, securities, personal property, real estate, and retirement accounts) and subtract your liabilities (or what you owe in loans and other obligations).

# Independence Policies on Investments

Any direct financial interest by a covered person and their immediate family members, in a restricted entity, no matter how small it is or how long ago it was purchased, impairs their independence. See also exceptions to this rule on slide 26 of this document related to spousal benefit plans.

An indirect investment by a covered person and their immediate family members, in a restricted entity impairs their independence if it is material to their net worth. See also exceptions to this rule on slide 26 of this document related to spousal benefit plans.



An indirect investment by a covered person and their immediate family members, in a restricted entity impairs their independence only if it is material to their net worth.

## Remember

Check investments holdings before you begin work on an audit client, talk to the Engagement Partner if you have any investments in the audit client or its affiliates.

# Independence Policies on Loans

Your personal independence may be affected if you, or an immediate family member, has or is thinking about making an investment, obtaining a loan or entering into other financial relationships.

Like investing, borrowing money from a restricted entity creates a financial relationship between you and the entity that could potentially impair your independence. Accordingly, the CPA Code and the SEC have rules and requirements governing loans.

The IESBA Code generally allows covered persons to obtain loans from a restricted entity that is a bank or similar institution, provided the loan is obtained under normal lending procedures, terms and requirements.

This document explores KPMG's policies on loans.



## SEC Restricted Entities

SEC rules are significantly more restrictive than the IESBA Code. The SEC rules prohibit any KPMG covered person (and their immediate family members) from having a loan (including margin loans) to or from a SEC audit client, any officers or directors, or any record or beneficial owners owning 10% or more of a restricted entity, with some exceptions (i.e. grandfathered loans, certain collateralized loans).



## Restricted Entities include:

- An audit or assurance client
- 'Affiliates' of an SEC audit client
- 'Related entities' of an IESBA audit client.

# Independence Policies on Loans

## Non-SEC Restricted Entities

### Who is affected?

Covered persons and their immediate family members. Refer to "Covered Persons" slide for more information on who is considered a covered person.

### What loans are prohibited?

Any loans from a restricted entity that is not a bank or similar institution.

### What loans are permitted?

Covered persons may obtain loans from a restricted entity that is a bank or similar institution provided the loan is obtained under normal lending procedures, terms and requirements. Examples of such loans include home mortgages, bank overdrafts, car loans and credit card balances.

### Are there any “grandfathering” provisions?

No

# Independence Policies on Loans

## Non-SEC Restricted Entities

### Who is affected?

Covered persons and their immediate family members. Refer to "Covered Persons" slide for more information on who is considered a covered person.

### What loans are prohibited?

A covered person and their immediate family members may not have any loan (including any margin loan, such as a loan taken out from a broker to finance the purchase of securities) to or from a restricted entity, its officers or directors, or any record or beneficial owners owning more than 10% of a restricted entity (except those loans specifically permitted below).

Prohibited loans include student loans.

### What loans are permitted?

Covered persons may obtain:

- Automobile loans/leases collateralized by the automobile
- Loans fully collateralized by the cash surrender value of an insurance policy
- Loans fully collateralized by cash deposits at the same financial institution

### Are there any “grandfathering” provisions?

Generally, a “grandfathered” loan is a loan on your primary residence that would not be in compliance with today’s independence rules, but is still allowed because it was permitted at the time the transaction occurred.

# Independence Policies on Loans

## Non-SEC Restricted Entities

### Under what conditions would my loan with an SEC restricted entity be grandfathered?

Your mortgage loan (including second mortgages, home improvement loans, home equity lines of credit and similar obligations) with an SEC restricted entity meets the conditions for grandfathering if it is collateralized by your PRIMARY residence and if you obtained it under any of the following conditions:

You obtained the loan before you became a covered person

You obtained the loan before the financial institution became a restricted entity

You obtained the loan from a non-restricted financial institution (including loans originated by a mortgage broker) that was later sold to a restricted entity

Mortgages on second homes or investment properties may not be grandfathered.

In addition, any loan that you obtained before May 7, 2001 qualifies for grandfathering, assuming it was permitted under the existing independence standards as of that date.

### May I make changes to my grandfathered loan?

No!

Your loan would no longer be considered grandfathered if you change the terms of the loan in any manner not provided for in the original loan agreement. Changes in the terms of the loan include, but are not limited to:

- A new or extended maturity date
- A new interest rate or formula
- Revised collateral, or revised or waived covenants

After the grandfather date, a loan or line of credit balance may only be reduced. You are not permitted to re-borrow amounts paid off.



# Independence Policies on Loans

Your personal independence may be affected if you, or an immediate family member, has an investment, obtains a loan or enters into other financial relationships.

Do you have any of the following: bank accounts, brokerage accounts and futures commission merchant accounts, credit cards, insurance policies, or spouse and dependent benefit plans?

In general there are no restrictions on these relationships for non-SEC restricted entities as long as the relationships are with a bank, broker or similar institution, and are on normal commercial terms and conditions, and are generally available to the public. In the case of spouse and dependent benefit plans, certain other conditions apply – and these are explained later in this document.

If you are not a covered person you are not subject to these rules.



## SEC Restricted Entities

If you are a covered person, any of the relationships, outlined in this document, with an audit client (restricted entity) must comply with the independence rules. The SEC has specific tests and conditions for each type of financial relationship listed at the left.



## Restricted Entities include:

- An audit or assurance client
- 'Affiliates' of an SEC audit client
- 'Related entities' of an IESBA audit client.

# Independence Policies on Other Financial Relationships

## Non-SEC Restricted Entities

In general, covered persons and their immediate family members are not restricted from having 'other financial relationships' with non-SEC restricted entities as long as the relationships are:

with an entity that is a bank, broker or similar institution

on normal commercial terms and conditions

generally available to the public

### Exception:

The IESBA Code does have specific requirements for spouse and dependent benefit plans similar to those of SEC restricted entities. See the next tab for those rules.

# Independence Policies on Other Financial Relationships

## Spouse and Dependent Benefit Plans

The holding – through a spousal/dependent benefit plan – of a financial interest in a restricted entity which would otherwise be prohibited is permitted if the following conditions are met:

The financial interest is received as a result of the immediate family member's employment rights, for example, through pension or share option plans

When necessary, safeguards are applied to eliminate any threat to independence or reduce it to an acceptable level

However, when an immediate family member has or obtains the right to dispose of the financial interest, or the right to exercise a stock option, the financial interest must be disposed of or forfeited as soon as practicable (which, in this context, means within 30 days).

Covered persons that are members of the audit engagement team, are NEVER permitted to have investments (including vested and unvested stock options) in a restricted entity through a spousal/dependent's benefit plan or otherwise.

If your immediate family members have investments in an audit client through a benefit plan please notify the Lead Audit Partner prior to performing any service.

# Independence Policies on Other Financial Relationships

## Bank Accounts



**Note:** Non-SEC restricted entities have no specific requirements relating to this topic. See the Non-SEC Restricted Entities tab for general information.



The REGULATOR protects depositors against the loss of their insured deposits if a X-insured bank or saving association fails.

**Notes:**

Foreign currency accounts held in COUNTRY ARE/ARE NOT insured by the REGULATOR.

### SEC Restricted Entities

If you are a covered person, you and your immediate family may not have a depository account\* balance in excess of FDIC (Federal Deposit Insurance Corporation)\*\* (\$250,000 FDIC limitation for US) or equivalent non-US insured limits.

\* Depository accounts include savings and chequing accounts

\*\*Insured savings are calculated by combining balances in certain types of accounts (e.g. savings and chequing accounts).

You must continuously maintain the depository accounts within the insured limits, even within the course of a single day. Any overdraft protection must be tied to a credit card or savings account. (Note: overdraft protection tied to a credit card or savings account may not be available in your country.) Overdraft protection cannot be tied to a line of credit or loan. Overdraft protection is not available everywhere; an arrangement with your bank to offset your overdraft against a savings account balance for the purposes of calculating interest is not prohibited.

# Independence Policies on Other Financial Relationships

## Broker-Dealer Accounts



**Note:** Non-SEC restricted entities have no specific requirements relating to this topic. See the Non-SEC Restricted Entities tab for general information.

A **broker-dealer** is a company or other organization that trades securities for its own account or on behalf of its customers. When executing trade orders on behalf of a customer, the institution is said to be acting as a broker. When executing trades for its own account, the institution is said to be acting as a dealer.

### SEC Restricted Entities

If you are a covered person, you and your immediate family members are permitted to maintain **broker-dealer** accounts with SEC restricted entities, as long as the balances do not exceed the insured limit specified by **SIPC** ((currently a maximum coverage of US\$500,000 per insured account including up to US\$100,000 for cash) or equivalent non-US insured limits.

### *Futures Commission Merchant Accounts*

KPMG member firms, covered persons and their immediate family members shall not have futures commission merchant accounts (including any futures, commodity, or similar account maintained with a futures commission merchant) with an SEC restricted entity.



### **SIPC (Securities Investor Protection Corporation):**

Protects customers of broker-dealers (as long as the broker-dealer is a SIPC member) if a brokerage firm is closed due to bankruptcy or other financial difficulties and customer assets are missing. SIPC steps in and works to return most customers' cash, stock and other securities.

# Independence Policies on Other Financial Relationships

## Broker-Dealer Accounts



**Note:** Non-SEC restricted entities have no specific requirements relating to this topic. See the Non-SEC Restricted Entities tab for general information.

### What if my brokerage account includes a money market mutual fund?

Brokerage accounts may be set up to include a money market mutual fund established by the broker. This fund may be used to hold temporary cash such as customer deposits.

It is also used to automatically “sweep” proceeds from security sales and dividend and interest receipts. These money market mutual funds are considered investments for independence purposes. Similar to any other prohibited investment, an investment in a restricted money market mutual fund is prohibited under firm independence policies and must be disposed of prior to providing any services to the client (i.e. before you become a covered person).

### Can I have a margin account with my broker?

Margin accounts are considered loans. Covered persons and their immediate family members are prohibited from having margin loans with restricted broker-dealers.

**Margin accounts:** The broker-dealer may allow you to borrow money to buy additional securities.

# Independence Policies on Other Financial Relationships

## Credit Cards



**Note:** Non-SEC restricted entities have no specific requirements relating to this topic. See the Non-SEC Restricted Entities tab for general information.



### SEC Restricted Entities

If you are a covered person, you and your immediate family members are permitted to have credit cards (including cash advances and checking account overdraft protection arrangements tied to a credit card) from a restricted entity provided the current outstanding balance is reduced to US\$10,000 or less by the payment due date. Balances are permitted to exceed this limit during the credit card cycle.

You must aggregate credit card balances with the same restricted entity when evaluating the US\$10,000 limitation. You must also include the accounts of immediate family members and ensure all amounts outstanding are current.

Note: 'balance' for this purpose is calculated at the current exchange rate.

# Independence Policies on Other Financial Relationships

## Credit Cards



**Note:** Non-SEC restricted entities have no specific requirements relating to this topic. See the Non-SEC Restricted Entities tab for general information.



### SEC Restricted Entities

If you are a covered person, you and your immediate family members may not obtain an individual insurance policy issued by an SEC restricted entity.

An existing policy is considered grandfathered (and will not create an independence violation) if you maintain or renew a policy that was either:

- Obtained before May 7, 2001 or before you became a covered person
- If the likelihood is remote that the insurer will become insolvent

You may not increase coverage on an existing policy unless increases are in accordance with pre-existing contractual terms.

Variable life and variable annuity contracts issued by insurance companies function as investment vehicles, as the value is determined by the performance of the underlying investments. Covered persons and their immediate family members shall not hold variable life and variable annuity contracts issued by an SEC restricted entity. These variable contracts cannot be grandfathered and must be either disposed of, or converted to a fixed annuity, upon becoming a covered person.

# Non-Audit Services — IESBA

The IESBA Code of Ethics is the KPMG International baseline for independence requirements and the application of the rules differ between public interest entity audit clients and non-public interest entity audit clients. The rules on non-audit services are detailed and include ten specific categories of services that will, if specifically prohibited or if there are insufficient safeguards to reduce the threats to independence, would result in a breach of professional standards, and therefore also of Firm policies:

- Accounting and Bookkeeping Services
- Administrative Services
- Valuation Services
- Internal Audit Services
- Information Technology Systems Services
- Tax Services
- Litigation Support Services
- Legal Services
- Recruiting Services
- Corporate Finance Services

In addition, there is an absolute prohibition on assuming a management responsibility.

However, if any of the above services are provided to non-audited parent or sister entities and if it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements, they may be permissible

Firm independence policies prohibit an individual, a member firm, or any entity that is associated with a member firm, a partner, or a professional employee of a member firm through ownership, influence, control or otherwise (including entities associated with immediate family members) from providing the above prohibited non-audit services to an audit client.

Please note that the rules for non-audit services are complex and vary depending on whether the client is regarded as a public interest entity audit client or a non-public interest entity audit client.

**If you been requested to perform one of these services, please consult with the Engagement Partner to ensure service is permissible.**

# Non-Audit Services — US SEC

The US SEC independence requirements for reporting issuers are detailed and include ten specific categories of services that, if provided to a reporting issuer audit client, would result in a violation of professional standards, and therefore also of Firm policies:

1. Bookkeeping and related type services (including Payroll and Cash Handling)
2. Financial Information Systems Design and Implementation
3. Appraisal and Valuation Services
4. Actuarial Services
5. Internal Audit outsourcing
6. Management Functions (including Loaned or Seconded Personnel)
7. Human Resources Services (including Recruiting)
8. Broker-Dealer or other investment advisory type services
9. Legal Services (including Corporate Secretarial)
10. Expert Services (including Litigation Support)

Of these ten non-audit service categories, the first five may not result in an independence violation if it is reasonable to conclude that the results of these services will not be subject to audit procedures during an audit of the audit client's financial statements.

This exception only applies when the Firm does not audit the parent company and the service is provided to a sister company or, in certain situations, the parent company of our audit client.

However consultation with the KPMG CIS Ethics and Independence team is encouraged in making this assessment.

**Non-audit services (6) through (10)** are not subject to this exception and, as a result, may never be performed for a reporting issuer audit client or its affiliates.

Firm independence policies prohibit an individual, a member firm, or any entity that is associated with a member firm, a partner, or a professional employee of a member firm through ownership, influence, control or otherwise (including entities associated with immediate family members) from providing the above prohibited non-audit services to a reporting issuer audit client.

Please note that the rules for non-audit services are complex and vary depending on whether the client is regarded as a reporting issuer audit client or non-reporting issuer audit client.

**If you been requested to perform one of these services, please consult with the Engagement Partner to ensure service is permissible.**

# Additional KPMG independence requirements for Ukraine



## Ukraine

**Relatives:** adopted children (inc. stepchildren), adoptive parents (inc. stepparents), [great-] grandchildren, [great-]grandparents, cousins, uncles, aunts, nephews, nieces as well as parents and siblings of a spouse as well as sons-in-law and daughters-in-law and their parents, inc. other cohabitants sharing housekeeping and reciprocal rights and obligations

The Law of Ukraine on Audit of Financial Statements and Auditing activity prohibits immediate, close family members and Relatives as outlined above of auditors, KPMG Ukraine audit partners and directors, members of KPMG Audit JSC governing bodies and its beneficiaries:

- holding financial instruments issued by their audit client/ an entity sharing common property or under common control/governance with the audit client
- being engaged in transactions with financial instruments, issued, guaranteed or otherwise backed by the audit client
- during the audit and the period covered by the audit having employment, contractual or other relations with the audit client which may create a conflict of interest (e.g. the conflict is created if an auditor was involved in preparation of or taking management decisions for the audit client)

In addition, the Law prohibits all audit team members, KPMG Ukraine audit partners and directors, members of KPMG Audit JSC governing bodies taking up key management positions, becoming members of administrative, management or supervisory bodies, members of audit committees or similar for:

- non-PIE audit clients within at least one year after they ceased to act in their above capacity
- PIE audit clients within at least two years after they ceased to act in their above capacity

The Law of Ukraine on valuation of Property, Property Rights and Professional Evaluation Activity in Ukraine prohibits immediate, close family members of appraisers (and management of the valuation firm) as well as parents, siblings and children of their spouses being their valuation clients or being their valuation clients' management.

# Resources

If you are uncertain about whether you can work on a client where you hold:



**Financial interests**  
(e.g. stocks, bonds and mutual funds)



**Financial relationships**  
(e.g. loans, credit cards, savings account, brokerage accounts and RRSP)

You should discuss your concerns with the engagement partner prior to doing any work.

You can also contact the KPMG ~~GIS~~ Ethics and Independence team



# Data Privacy Training

# Let's do this

# Welcome to the Data Privacy Training

## Learning objectives:

This course will give you the fundamental skills and knowledge to help you understand data privacy, enabling you to protect our information, our clients' information and KPMG's reputation.

## Completing this course will help you to understand:

- Why looking after Personal Data is so important
- The guidelines that underpin how we must look after Personal Data and follow legal requirements
- What Impact it has on the way we work
- What to do if there is a breach
- The Framework supporting transfers of Personal Data between KPMG member firms

In our everyday lives, we share massive amounts of information about ourselves with other people, businesses and governments. For example, in order to do personal banking or obtain a credit or debit card, you must share Personal Data with the banking institution. You might be more sensitive about some pieces of information than others.

Regardless of the information's sensitivity though, you would probably still expect the bank to look after all your information and protect it properly. In fact, the bank is legally obliged to look after your Personal Data and treat it in accordance with applicable data privacy legislation.

In the same way that the bank holds your Personal Data, KPMG holds Personal Data about people, including employees, contractors, work experience students, clients or their employees, or individuals who interact with KPMG in other ways, such as via a public-facing website.

# Why it's important to protect Personal Data?

In the process of work, we obtain access to Personal Data from both our colleagues and KPMG clients. Some persons may also need to work with special categories of Personal Data.

**Personal Data includes information or a set of information about an individual who is identifiable or can be specifically identified;)\* :**

Name, address, date of birth, email address, phone number, racial background, intimate information, favorite chocolate brand/smart phone app, foreign language skills, profession, etc.



**\*Law of Ukraine “On Personal Data Protection” dated 1 June 2010**

Special Personal Data categories include information on racial or ethnic origin, political, religious or ideological beliefs, membership in political parties and trade unions, criminal convictions, and data relating to health, sexual life, biometric or genetic data. The above examples represent special categories of Personal Data, since they characterize the confidentiality of the subjects and can be used in a discriminatory manner. Special categories of Personal Data require even more careful processing than other Personal Data.

Before processing special categories of Personal Data, we must obtain a written consent of the subject of such data. Only employees of certain KPMG departments have the right to handle special categories of data. If you have any doubts or questions, please consult Privacy Liaison responsible for processing of Personal Data in KPMG (see contacts presented in the end.)

# Why it's important to protect Personal Data?

## Responsibility for violation of the legislation on Personal Data protection

### Administrative liability

(Article 188-39 of the Code of Ukraine on Administrative Offenses):

1. Failure to submit or late submission to the Verkhovna Rada's Authorized Person for human rights about processing of Personal Data or changes in the data that must be made available in accordance with the effective law, submission of incomplete or unreliable information.
2. Failure to comply with legal requests (orders) of the Verkhovna Rada's Authorized Person for human rights or requests (orders) or the officers authorized by the Authorized Person to the Secretariat of the Verkhovna Rada's Authorized Person for human rights as regards prevention or elimination of the laws on Personal Data protection.
3. Failure to comply with the established by the legislation procedure for protection of Personal Data resulted in illegal access to the data or violation of the rights of a Personal Data subject.

### Criminal liability

(Article 182 of the Criminal Code of Ukraine):

Illegal collection, storage, use, destruction, dissemination of confidential personal information or illegal alteration of such information, except as provided by other articles of Criminal Code of Ukraine.

### Disciplinary liability

(article 10 of the Law of Ukraine "On Personal Data Protection"):

Use of Personal Data by employees of entities related to personal data shall be only if required by their professional, official or labor duties. These employees are obliged to prevent disclosure in any way of the Personal Data entrusted to them or which became known in connection with the performance of professional or official or labor duties unless otherwise is stipulated by the law. This obligation remains valid after their termination of activities related to personal data unless otherwise is stipulated by the law.

# Why is looking after Personal Data so important?

## Failing to protect Personal Data: the financial and legal consequences

In May 2018, the General Data Protection Regulation (GDPR) transformed the data protection landscape with the biggest shake-up in data protection legislation in over 20 years.

It focuses extensively on ensuring data subjects know, understand and agree to exactly what their data is being used for. It strengthens their rights.

- Individuals – The GDPR gives people greater control of their Personal Data and how it is used.
- Businesses – The GDPR enhances the way we work with and manage Personal Data.

## Other consequences of failing to protect Personal Data

The financial and legal consequences of failing to protect Personal Data can be measured and quantified.

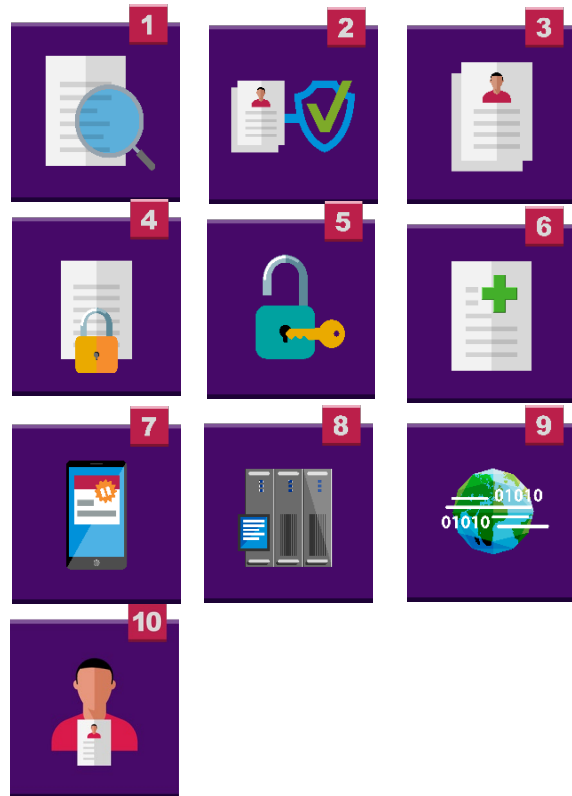
Reputational damage is not so easily predicted. Trust is hard earned, but it is so easy to lose. It is a two-way street built upon competent, safe and secure practices.

If we fail to protect our clients' data, we risk losing their trust and their business.

If you discovered your favorite supermarket had compromised your Personal Data, you'd probably consider going elsewhere. Finally, we risk opening ourselves up to increased scrutiny from regulators, which will require time and effort from all of us.

# How We Must look after Personal Data and Sensitive Personal Data

If you are working with Personal Data, you must ensure you follow KPMG's 10 Data Privacy Principles to ensure we comply with data privacy law.



## KPMG's 10 Data Privacy Principles

### 1. Transparency

KPMG member firms will tell individuals how we process their Personal Data – to the extent necessary to ensure that processing is fair.

### 2. Purpose Limitation

KPMG member firms will only process Personal Data for the purposes:

- set out in any notices, made available to the relevant individuals, which are relevant to KPMG;
- as required by law; or
- where consented to by the relevant individuals
- where the relevant individuals have given their consent

You can find out why the Personal Data are being collected in the consent form provided by the individual, or in other materials where the processing purpose has been declared (for example, engagement contracts or any other agreements with a client).

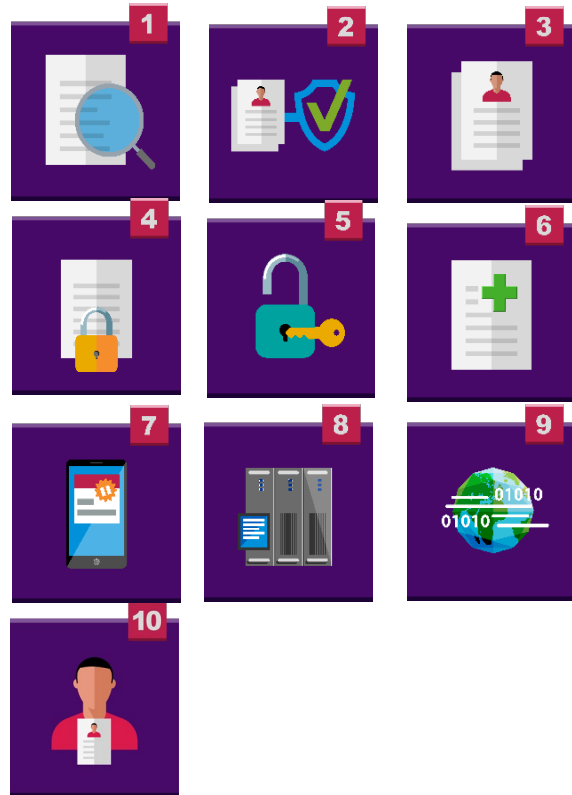
If you intend to use Personal Data to attain a secondary purpose (in other words, other than the primary purpose previously declared for their collection), follow the [GIS](#) guidance on secondary use of personal data - you must first notify the individual/client/third party and obtain their consent.

### 3. Data Quality and Proportionality

Personal Data should be kept accurate and, where necessary, up to date. The Personal Data KPMG member firms hold must be adequate, relevant and not excessive. The period of information storage should not exceed the period necessary for the relevant purpose of Personal Data processing.

# How We Must look after Personal Data and Sensitive Personal Data

If you are working with Personal Data, you must ensure you follow KPMG's 10 Data Privacy Principles to ensure we comply with data privacy law.



## KPMG's 10 Data Privacy Principles

### 4. Security and Confidentiality

Reasonable precautions must be taken to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access.

These precautions should include technical, physical and organizational security measures that are commensurate with the sensitivity of the information and the level of risk associated with the processing of it. From time to time, the applicable measures may be documented more fully in IT and risk management policies adopted by the KPMG member firms.

Where necessary or appropriate, KPMG member firms must consider implementing additional measures for particular types of Personal Data that may need to be handled with additional care, so as to respect local customs, laws or regulations. This may include Sensitive Personal Data.

Where a KPMG Firm processes Personal Data on behalf of another KPMG Firm, it will only act under the first firm's instructions

KPMG employees may only disclose Personal Data in cases where it has been established that:

- a written or other form of consent permitted by law has been obtained from the employee / client / third party prior to the disclosure, except in instances where the receipt of such consent is not stipulated by the law;
- the disclosure of such information is stipulated by the applicable law or professional standards (for example, local legislation on auditing); or
- the disclosure is binding by virtue of the requirements of law, state authority or decision of the court.

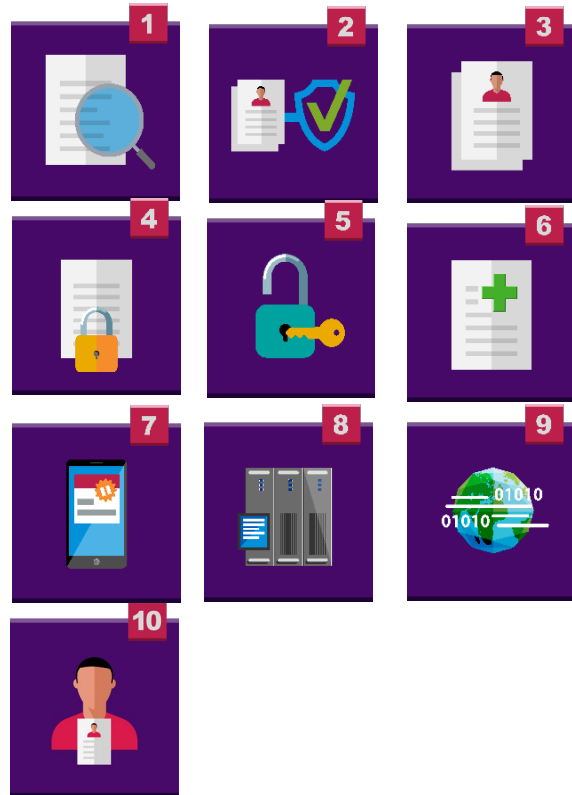
### 5. Access, Rectification, Deletion and Objection

Individuals should have access to their Personal Data that is held by KPMG member firms, where those requests are reasonable and permitted by law or regulation. KPMG member firms agree to rectify, amend, or delete Personal Data upon request where it is inaccurate or where it is being used contrary to these key principles.

An individual should be able to object to the processing of their Personal Data if there are legitimate grounds relating to their circumstances.

# How We Must look after Personal Data and Sensitive Personal Data

If you are working with Personal Data, you must ensure you follow KPMG's 10 Data Privacy Principles to ensure we comply with data privacy law.



## KPMG's 10 Data Privacy Principles

### 6. Sensitive Data

Where KPMG member firms process Sensitive Personal Data, they will take such additional measures as are necessary to protect that data.

### 7. Data Used for Marketing Purposes

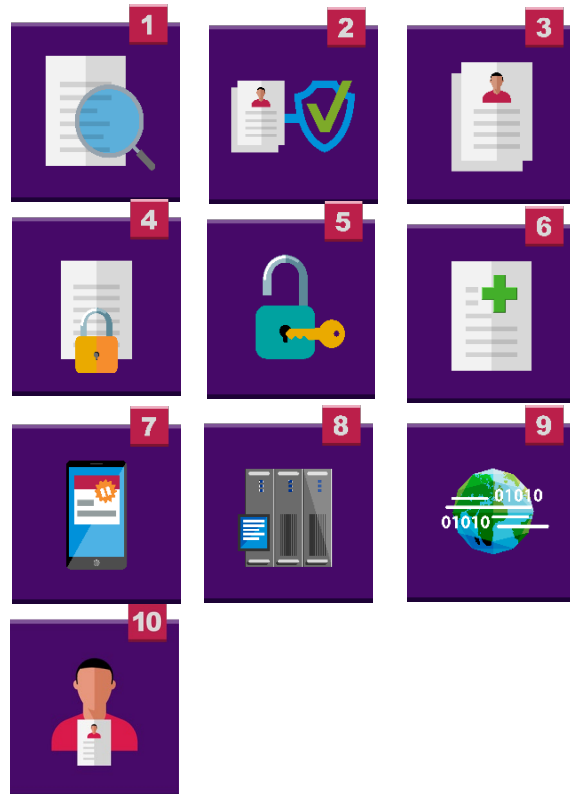
Where data is processed for the purposes of direct marketing, effective procedures should exist allowing the person at any time to "opt-out" from having their data used for such purposes.

### 8. Automated Processing

Where KPMG member firms process Personal Data on a purely automated basis that has a legal or significant impact on an individual, those KPMG member firms shall give the individual the opportunity to discuss the output of such processing before making those decisions.

# How We Must look after Personal Data and Sensitive Personal Data

If you are working with Personal Data, you must ensure you follow KPMG's 10 Data Privacy Principles to ensure we comply with data privacy law.



## KPMG's 10 Data Privacy Principles

### 9. Information Transfer and Compliance

Within the global network of KPMG member firms, Personal Data may be transferred outside the country in which it was collected, including countries outside of the European Economic Area (EEA), for legitimate business activities.

In addition, the KPMG member firms may store Personal Data in facilities operated by other KPMG member firms and/or third parties on behalf of the KPMG member firms outside the country in which the data was collected.

Nevertheless, Personal Data must not be transferred to another country unless the transferor has assurance that an adequate level of protection is in place. An adequate level of protection is ensured by the Inter-Firm Agreement about Data Protection which each KPMG member firm must comply with.

KPMG member firms will ensure that where Personal Data is transferred to third parties outside of the KPMG network for processing, this is only done where the Personal Data is adequately protected.

### 10. Data Minimization

Where KPMG member firms retain individuals' Personal Data, those KPMG member firms will do so in a form identifying or rendering an individual identifiable only for so long as it serves the purpose(s) for which it was initially collected or subsequently authorized except to the extent permitted by law.

# How We Must look after Personal Data and Sensitive Personal Data

## The role of Data Controller and Data Processor in applying our Principles

A further aspect of data privacy legislation is the notion of the Data Controller and the Data Processor.

KPMG is a Data Controller when it processes the data of employees and contractors (whether prospective, current or past) or individuals whose data we hold for marketing purposes. **KPMG is responsible for compliance with all of KPMG'S Data Privacy Principles.**

When performing engagements for clients, KPMG may act as a Personal Data Controller or Personal Data Processor depending on the specific circumstances or type of engagement specified in the contract with the client. Personal Data Processor may process Personal Data only for the purpose and to the extent specified in the engagement contract.

### Data Processor



natural or legal person authorized by the Personal Data Controller or by the law to process this data on behalf of the Controller;

### Data Controller



natural or legal person, which determines the purpose of processing Personal Data, establishes the composition of this data and the procedures for its processing unless otherwise is stipulated by the law;

### Remember

Following KPMG'S 10 Data Privacy Principles will help you to meet your obligations to the client.

# What Impact does Data Privacy have on How you Work?

## Do not collect more data than you need

Accidental data breaches often occur when data is being collected. It is one of the most common inadvertent data breach scenarios. If you are working with a client and you need to obtain client data, you may end up collecting more than you need. This presents a risk and it breaches one of KPMG's 10 Data Privacy Principles: Data Quality and Proportionality.

You must communicate with the client to ascertain precisely what data you need. If you are sent more than you require, you must tell the client. You must then delete it or send it back. You must also work with the client to ensure the data is both relevant and accurate.

## Send data securely

Trust can take a long time to earn. It can be lost so quickly. Our clients entrust us with their most sensitive data and we are all obligated to safeguard it. We can reduce the possibility of data loss by ensuring the data we are sending is appropriate and sent to the correct individual. **Here are some tips:**

- Stop and think before sending confidential information via email. Investigate the possibility of using KPMG Central.
- When emailing confidential files, you should encrypt them and send the password separately.
- Double check the recipient, especially on email. Autocomplete is useful but often leads to breaches.
- When temporarily transferring data, you should use KPMG approved devices and keep them secure at all times.

## Keep information secure when traveling

Mobile working presents a lot of risks. Minimize these risks by reducing the amount of data you take with you and avoid carrying hard copies where possible. If you do require hard copies, take only what is absolutely necessary. Never leave your laptop in standby mode when traveling. Ensure it is fully shut down.

## Understand client permissions

Your client engagement letter dictates how you use data. During your engagement, periodically carry out reviews on the data you have collected to check whether it is still required.

## Retain information in the right place

KPMG may be subject to fines and reputational damage if we store information inappropriately or fail to preserve information, data or devices. Follow these steps to make sure you are retaining information in the right place:

- Destroy information once its retention period passes, or as soon as is reasonably possible, except when there is a legal requirement to keep the data for longer.
- Retain information using approved methods as described in local policy or as requested by your Functional Risk Group.
- Familiarize yourself with KPMG's retention schedule.

# What Impact does Data Privacy have on How you Work?

## Do not secretly make multiple copies of client data in case you lose it

You must communicate with the client to ascertain what data you need. If you receive too much, you must inform the client and then delete it or send it back. Never make additional copies of data without authorization.

## Do not share positive experiences involving highly sensitive client work on social media

Never discuss client work on social media, unless you have been authorized to do so. What goes online, stays online. Remember it can never be truly erased.

## The Principle: Access, Rectification, Deletion and Objection

The data privacy principle of Access, Rectification, Deletion and Objection means that when working on client engagements there may be situations where individuals exercise their privacy rights.

For example, you may get a complaint from an employee of the client who is unhappy that KPMG are using their Personal Data as part of an engagement.

This may come directly to you, or via a Data Subject Access Request. If you receive either then you should inform the engagement partner and contact your Local Privacy Liaison who will be able to advise on the appropriate next steps.

## Marketing – Purpose Limitation

Obtain permission before sending materials to an individual. GDPR dictates that individuals must take action to opt-in to receive communications. This may take the form of ticking an unticked box.

Just because we hold someone's details, this does not mean we are free to casually distribute marketing emails to them. Careful consideration must be given before sending out marketing communications.

Ensure your direct marketing communications contain links allowing the recipient to subscribe or opt-in if they wish

Do not telephone someone if they previously requested us to stop making these calls.

If you wish to query anything we've covered here, or if you're in any doubt, please reach out to your local marketing team and Local Privacy Liaison.

# What to do if there is a Breach?

## Scenarios of Data Breach

Where's your data going?



I've sent Personal Data to the wrong person. What should I do?

Is your device secure?



My KPMG laptop has been stolen! It contains Sensitive Personal Data, what should I do?

Who's watching you?



I was on the train this morning reading sensitive client information and there was a commuter looking over my shoulder at my screen. What should I do?

If you encounter or suspect a data breach the first thing you should do is report it in accordance with the firm's processes.

# What to do if there is a Breach?

## What is a security incident?

Any event that **may** compromise the confidentiality, privacy, integrity, or availability of our information or information systems.

- It could be the loss of a KPMG laptop or USB drive
- It could be a data breach from an unauthorized network access
- It could be a malware threat from clicking on an email link or attachment
- It could be that your login credentials have been revealed to someone else

Importantly, it does not have to be something that you **know** has happened. It can be just something that **causes you concern** that our information may be threatened.

## Who do I tell?

If it is client related, immediately let your Engagement Partner and Data Privacy team know. Gather as many details as you can and report immediately to ISS via Data Loss Tool. Do not talk to the client about the issue. Instead, wait for advice from the local Data Privacy team.

If it is not client related, gather as many details as you can and report immediately to ISS via Data Loss Tool.

## When do I report it?

As soon as possible.

Data breaches must be immediately reported according to your local member firm procedures. That way, the appropriate corrective actions can be quickly taken.

When you report the breach, you must provide all the facts. Ensure you respond to all follow-up queries promptly (maximum within **24-hours**) because KPMG is obligated to report certain breaches to regulators within 72 hours of occurrence.

 You are not alone!

There is a strong support network within KPMG who will advise and help manage the situation resulting in the best resolution for everyone involved.

**If in doubt – just shout!**

# What to do if there is a Breach?

## The requirements of the General Data Protection Regulation (GDPR)

**On 25 May 2018, the General Data Protection Regulation (GDPR) transformed the data privacy landscape with the biggest shake-up in compliance and regulation legislation in 20 years.**

The legislation means changes for businesses and the public in general.

We will all benefit from the additional protection and control over our Personal Data, but this means we need to develop our processes to ensure we are providing this protection and do not incur any penalties.



### For everyone

- More control over own data
- More rights over own data



### For businesses

- Include data privacy in design of processes
- Report breaches within 72 hours
- Face increased penalties (up to €20 million or 4% of annual turnover – whichever equates to the larger amount) for failing to protect Personal Data



# Information Protection Fundamentals

# What is the nature of the threat facing KPMG?

All information is valuable.

But our increasing reliance on sophisticated technology makes it ever more critical to us – and an ever more tempting target for those wanting to exploit it.

We need your help to protect our information from malicious parties. **They may include:**

## Organized criminals

Organized crime can be defined as serious crime planned, coordinated and conducted by people working together on a continuing basis.



# What is the nature of the threat facing KPMG?

## Hackers

Hackers are people who use computers to gain unauthorized access to data



# What is the nature of the threat facing KPMG?

## Activists

Activists are people who campaign to bring about political or social change



# What is the nature of the threat facing KPMG?

## State-sponsored groups

State-sponsored terrorism is government support of violent non-state actors engaged in terrorism



# What is the nature of the threat facing KPMG?



Today, such parties are part of a thriving ‘data extraction’ industry that is a significant threat.

**But where does our biggest threat come from?**

Those working at KPMG

This is not through malicious intent. Rather, it results from not understanding how to work in a secure manner.

This course will provide you with the knowledge and techniques you need to safeguard against that threat.

# Why are we a target and how can you help?

At KPMG, security isn't just about looking out for your own wellbeing. We gather, process and safeguard critically sensitive data for the world's foremost companies.

They need total confidence in us as trustworthy custodians.

**That means we take information protection very seriously:**

We have sophisticated software and systems to protect our assets



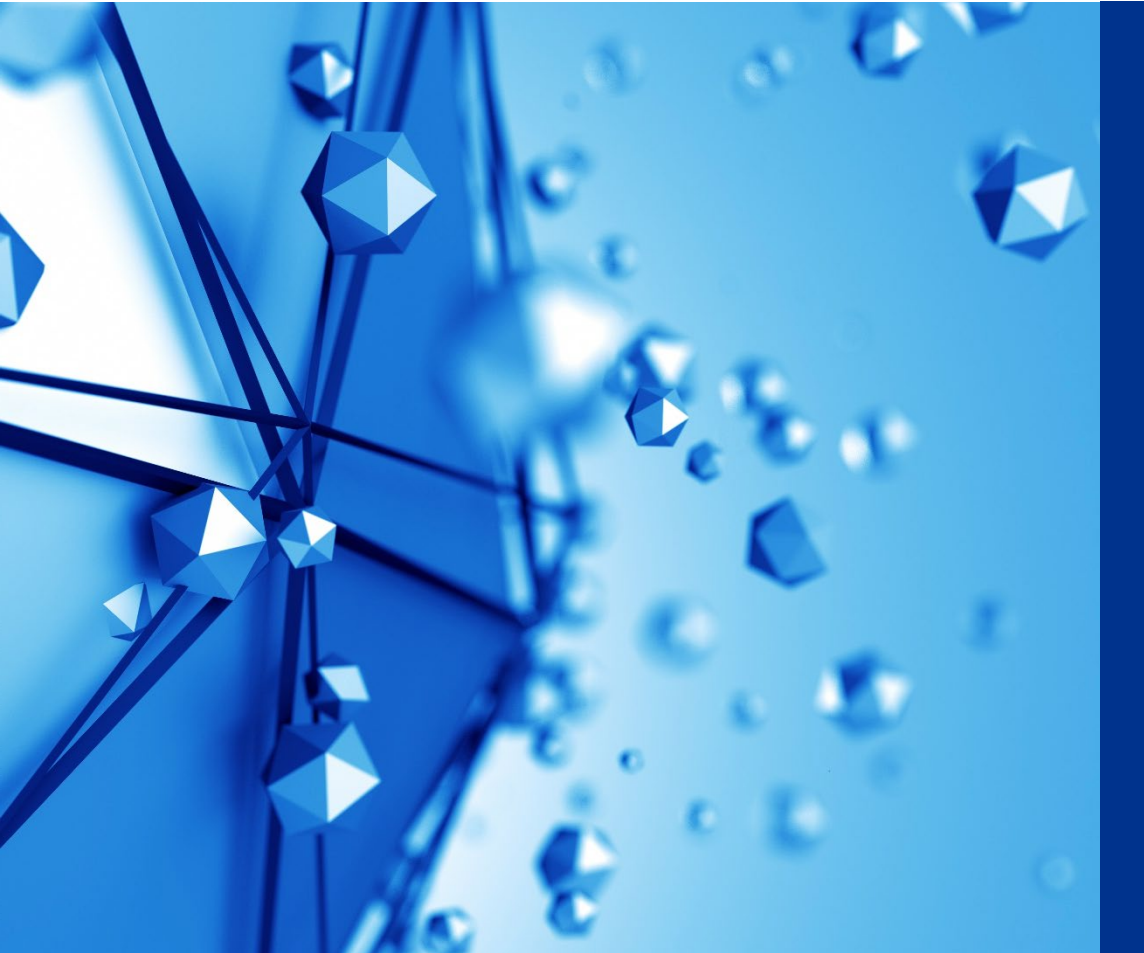
We have robust policies to securely handle our clients' data



We have a Global Security Operations Center (GSOC) that monitors for, and alerts member firms to, malicious attacks as they materialize



# Why are we a target and how can you help?



But these are nothing without our most important line of defense:

You

## How much is security worth?

Cyber crime cost is projected to reach a staggering £2 Trillion by 2019

*(Source: Juniper Research)*



# How does this affect me in my role at KPMG?

You can ensure you play your role in protecting our information by:



# How does this affect me in my role at KPMG?

If you fail to play your part, the consequences could be severe:

## Client



- Disruption to their use of our services
- Compromise of their most sensitive information
- Distress and difficulties for their employees
- Damage to their reputation and business
- Loss of their trust in KPMG

## KPMG



- Costs to put things right
- Imposition of regulatory penalties or fines
- Damage to our reputation and brand
- Loss of our license to operate as financial company
- Loss of the trust vital for our ongoing viability

So, it is important to take security seriously. It is your own, personal responsibility.

# Keeping to our values

The challenges we face in protecting our information are significant. But KPMG can build on a strong set of values that make us truly resilient.

**These are values shared across our member firms:**

## Independence

We are open and honest in our communication, managing tough situations with courage and candor.

**Report your security concerns promptly.**



# Keeping to our values

## Confidentiality

We maintain the confidentiality of client, firm and personal information at all times.

**Always think about the 'need to know', restricting information to only those who need it.**



# Keeping to our values

## Diligence

We seek the facts and provide insight, challenging assumptions.

**Take care to understand and follow local and global policies.**



# Keeping to our values

## Vigilance

We are committed to responsible stewardship of our firm's assets.

**Be on the lookout for threats and risks to those assets.**



# Keeping to our values

## Integrity

We act with complete integrity, complying with all applicable laws and regulations.

**Information protection relies on your integrity.**



Our values and ethics are built in to our Global Information Security and Global Acceptable Use Policies. These are the foundation of information protection at KPMG. Let's learn about some specific threats we face.

# Keeping vigilant against malware



There are many outside threats to be vigilant against. Malicious software (malware), especially ransomware, is one type of attack that has become increasingly common, costly and disruptive.

WannaCry is a recent example of a major ransomware cyber-attack, which seriously affected hospitals, car factories and power plants around the globe.

Once malware has infected a system it can disrupt business, enable fraud, compromise information and destroy reputations.

KPMG has a special responsibility for the prevention of malware and virus infections because of our day-to-day dealings with key companies worldwide.

You can help prevent malware attacks by undertaking due diligence and being extra vigilant. This is especially the case when dealing with emails, devices and downloading from the internet, as outlined in our Global Acceptable Use Policy.

# Keeping vigilant social engineering

Social engineering is another common attack. But what exactly is it?

01

It is a confidence trick that exploits human emotions

02

It may target you specifically using personal knowledge about you

03

It can be conducted through emails, on the phone or in person

04

It can happen at work or at home

05

It seeks to manipulate you for the attacker's benefit

06

It has no technical defense

A good example of social engineering, that most of us will have seen, is the sending of fake emails. This is often called phishing.

# What should raise your suspicions

Before you open or respond to any emails, even if apparently from your client or a firm colleague, there are some questions you should ask yourself. Click the red icons to see.

## Is the sender real?

The sender's email address might appear to be correct, but hovering over the 'From' shows it to be misspelt or an entirely different address.

## Does the link or attachment make sense?

An email might have a link whose URL is odd or mismatching, or an attachment might have an unusual format, such as a Microsoft Word document for an invoice.

## Does this belong here?

A sender might ask for, or provide, something you don't normally deal with, such as a purchase order or refund.

## Is the request appropriate?

Inappropriate requests include someone from IT asking for your password, or your lead partner asking for a transaction to be made immediately, against normal procedures.

## Is the sender behaving differently from before?

A familiar sender might address you using different language or ask odd questions.

A mocked-up image of an email and its preview page, with clickable elements highlighted by a question mark

If in doubt, then report the email:

Do not reply

Do not click on any links

Do not download any attachments



# Managing your devices



We aim to secure every part of our systems against attack. But we can only secure what we know about.

So, it is vital that you get approval before you work with devices such as laptops and phones. Using unapproved devices is a serious risk to the firm.

Only your local security officer (NITSO) can approve devices not supplied by KPMG, such as your own phone, for work.

# Managing your devices

Whether they are KPMG-supplied or approved, you must also take care to ensure that you:



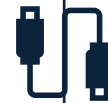
Secure devices out of sight when not in use; for laptops, use a security cable lock.



Sign off, lock the screen, or shut devices down and lock them out of sight if they will be left unattended for a long period.



Follow policies to remove sensitive information from the device when such information is no longer needed.



Only have devices repaired according to your firm's local ITS process.



Regularly connect KPMG-managed devices to our network so their defenses are kept up to date.



Return all KPMG-supplied devices and media when you leave the firm's employ.

# Vigilance starts when you arrive



Both at your member firm's premises and at our clients' offices, you will often have to use swipe cards, ID cards or passes to gain access to, or to move around, the building.

Sometimes, people may ask you to help them gain access through controlled doors. They may have forgotten their cards or they may be in a rush.

But this practice, sometimes called tailgating or piggybacking, is not secure.

To gain access, attackers exploit our instinct to help. Once inside, they could cause considerable harm.

By helping them, you are effectively handing them the keys to the building – and possibly our information.

So, politely refuse requests to help gain access, even where this may cause inconvenience to others. This is as simple as offering to take them to reception where they can get help.

# The challenge of challenging

Both within the member firm's premises and at client sites you need to maintain your vigilance when moving around.

Many such facilities make use of visible IDs. If the facility you're visiting uses such IDs, feel confident in challenging those not wearing one. This can be done in a polite and helpful manner.

If you ever see someone acting suspiciously, again feel confident in politely asking them why they are there. If they don't respond appropriately, you should report your worries to the local security team.

Don't forget, you will often be the stranger on the premises when working on site.

Always carry and wear appropriate ID and expect to be challenged. When this happens, be respectful and considerate in your responses.



# You'll need strong keys for systems, too



It's not just access to buildings and rooms that needs proper controls.

We also need you to create strong passwords to control access to our systems and protect our information.

Weak passwords are extremely vulnerable to 'dictionary attacks', which let attackers easily compromise your account. A weak password risks handing the keys to our systems and information over to those with malicious intent.

There are some simple rules in our Global Acceptable Use Policy.

Follow the rules on the next page to learn how to strengthen your passwords.

# You'll need strong keys for systems, too

01

They must be at least eight characters in length, and the longer you make them the more secure they will be

02

They should be made of two of more words combined

03

They should avoid common phrases found in film, literature or music

04

They must have at least three characters that are either upper case, lower case, numbers or special characters

05

They must not contain personal information such as your user name, real name, company name or dates of birth

# Which of these is strongest?

When you see each password, click on the label on the Strength-o-Meter that you believe matches its strength. The Strength-o-Meter will then indicate the actual strength of the password.

Very weak

password123

**Feedback:** This is one of the most commonly used (and easy to guess) passwords.

Weak

ThisPasswordIsStrong

**Feedback:** These words are linked in a common phrase and there are no special characters or numbers.

Strong

Th1sPa55wordisStr0ng

**Feedback:** The phrase is not easy to guess because of the use of numbers and a mix of cases.

Very strong

tPwDStr0nglt1s

**Feedback:** This phrase is disguised by dropping letters and including numbers and a mix of cases.

Strongest

T0matoGolfBa11EatsCars

**Feedback:** This phrase uses unconnected words, as well as numbers, a mix of cases and special characters.

# Keeping it confidential is critical

Confidentiality is key to every aspect of our business. The trust that our clients place in us, as guardians of their most sensitive information, is one of KPMG's greatest assets.

**You can play your part in 'keeping it confidential' by:**

Thinking carefully about the 'need to know'.

If available, using privacy screens on your laptop while in public.

Ensuring no information is left unattended on a desk or printer.

Disposing of confidential waste correctly.

Always connecting securely when not on KPMG premises.

Reporting incidents immediately, following your local procedures.

Being private when in public, whether traveling or working.

# Connect to KPMG Network from client



**My  
personal  
computer**

## Not allowed

You must never use an unapproved personal device to connect to KPMG Network from anywhere, including the client's office.



**My  
KPMG  
laptop**

## Requires specific approval

You can only connect to KPMG Network from the client's office with approval of your firm and your client.

# Sharing confidential information

## Cloud storage services

### Requires specific approval

You can only share files on approved cloud services with prior approval of your firm and your client.

## KPMG Central

### Requires specific approval

You can always share files using our collaboration site provided you set up and grant access to the site following proper procedure.

## My KPMG email

### Allowed

You should think carefully whether you need to send confidential information (including that belonging to clients) using email. Files are best shared using KPMG Central or other approved secure data transfer services.

## Encrypted USB Media

### Allowed

When using a USB device for transfer or backup of data, you must use only encrypted storage devices approved by KPMG.

## My personal email account

### Not allowed

To use a personal email account to share sensitive information.

## Personal cloud storage

### Not allowed

Never store confidential information in a personal cloud. You risk its integrity and security.

# Registering to LinkedIn or other social media



**My  
KPMG  
email**

**Not allowed**

You must never use your KPMG email accounts to register with non-work sites.



**My  
personal email  
account**

**Allowed**

It is fine to use your personal email accounts to register with non-work sites.

# Clearly secure?

We have a clear desk, clear screen policy at KPMG. That way we stop sensitive information from being seen by those who don't have a 'need to know'. Click on each highlighted area to see what you should do before you leave your desk unattended.

## Screen

You must lock your screen, so it is secured by a strong password, before leaving your desk.

## KPMG phone

Phones must be placed in a locked drawer or taken with you.

## Printer

Remove any printed documents from the printer and put them in a drawer. This should be locked if the information is sensitive.

## USB drive

Any storage device must be placed in a locked drawer or taken with you.

## Client's sensitive documents

Sensitive information must be locked away or disposed of in a confidential waste bin if no longer needed.

## Drawers and file cabinets

Make sure that cabinets that store sensitive data are locked at the end of each day.

# Taking care when working outside the office

Thinking about confidentiality doesn't end when you walk out of the member firm's premises or the client's door. You need to take great care wherever you are.

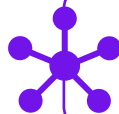
**When working outside of secure premises, make sure you protect our information by:**



Keeping your device with you at all times



Using a privacy screen, when provided, to avoid others being able to read your screen



Always use your KPMG VPN when working over a public Wi-Fi network

# Taking care when working outside the office

When you're talking to others outside of work, whether traveling, socializing or at home, remember to:



Never discuss any firm or client business



Never talk about your colleagues

Remember to show the same discretion when using social media. And don't reveal details of your employment and roles on business networking sites such as LinkedIn.


# If in doubt, report it

Keeping us all safe means making sure the right people know when you suspect a security incident.

## What is a security incident?

**Any event that may compromise the confidentiality, privacy, integrity, or availability of our information or information systems.**

- It could be the loss of a laptop or USB drive.
- It could be a data breach from an unauthorized network access.
- It could be a malware threat from clicking on an email link or attachment.
- It could be that your login credentials have been revealed to someone else.



Importantly, it doesn't have to be something that you know has happened. Just something that causes you concern that our information may be threatened.

# If in doubt, report it

## Who do I tell?

- If it is client related, immediately let your Engagement partner and Quality and Risk Management team know. Don't talk to the client about the issue. Instead, wait for advice from the local Quality and Risk Management team.
- If it is not client related, follow your local member firm's procedures. This will normally be handled by your local security department, unless the incident needs to be escalated.

## When do I report it?

- As soon as possible.
- Security incidents must be immediately reported according to your local member firm procedures. That way, the appropriate corrective actions can be quickly taken.

# Making sure you travel safety

Whenever and wherever you travel, you should always follow the core security principles outlined in this course:



# Making sure you travel safety



It's vital to protect our information when we travel. But we also want to protect you.

We have many resources available to help ensure your safety, including International SOS (ISOS), our principal global security support provider.

A smartphone app gives you access to all the International SOS resources.

Their website also provides the latest information on the security and medical situation in whichever country or city you are to visit.

You should also print your own International SOS card to carry with you at all times.



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



[kpmg.ua](https://kpmg.ua)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2022 KPMG-Ukraine Ltd., a company incorporated under the Laws of Ukraine, a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

**Document Classification: KPMG Confidential**