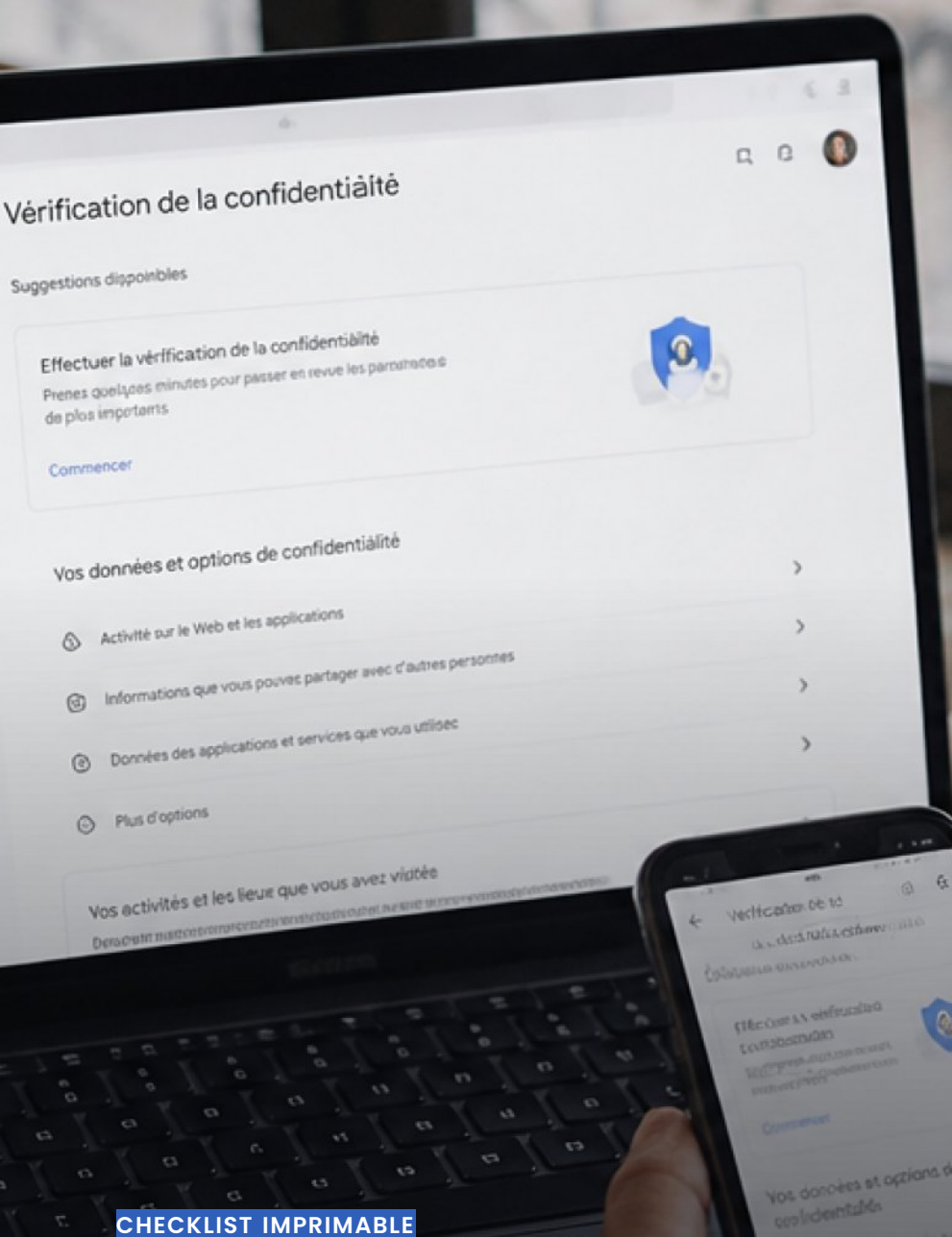




CHECKLIST IMPRIMABLE

Caméra et micro : la checklist pour reprendre le contrôle

Utilisez cette fiche pour repérer un accès inattendu, retirer les autorisations inutiles et vérifier que le blocage fonctionne. Caméra et microphone se règlent séparément : adaptez le niveau d'accès à l'usage réel de chaque application.

Au sommaire

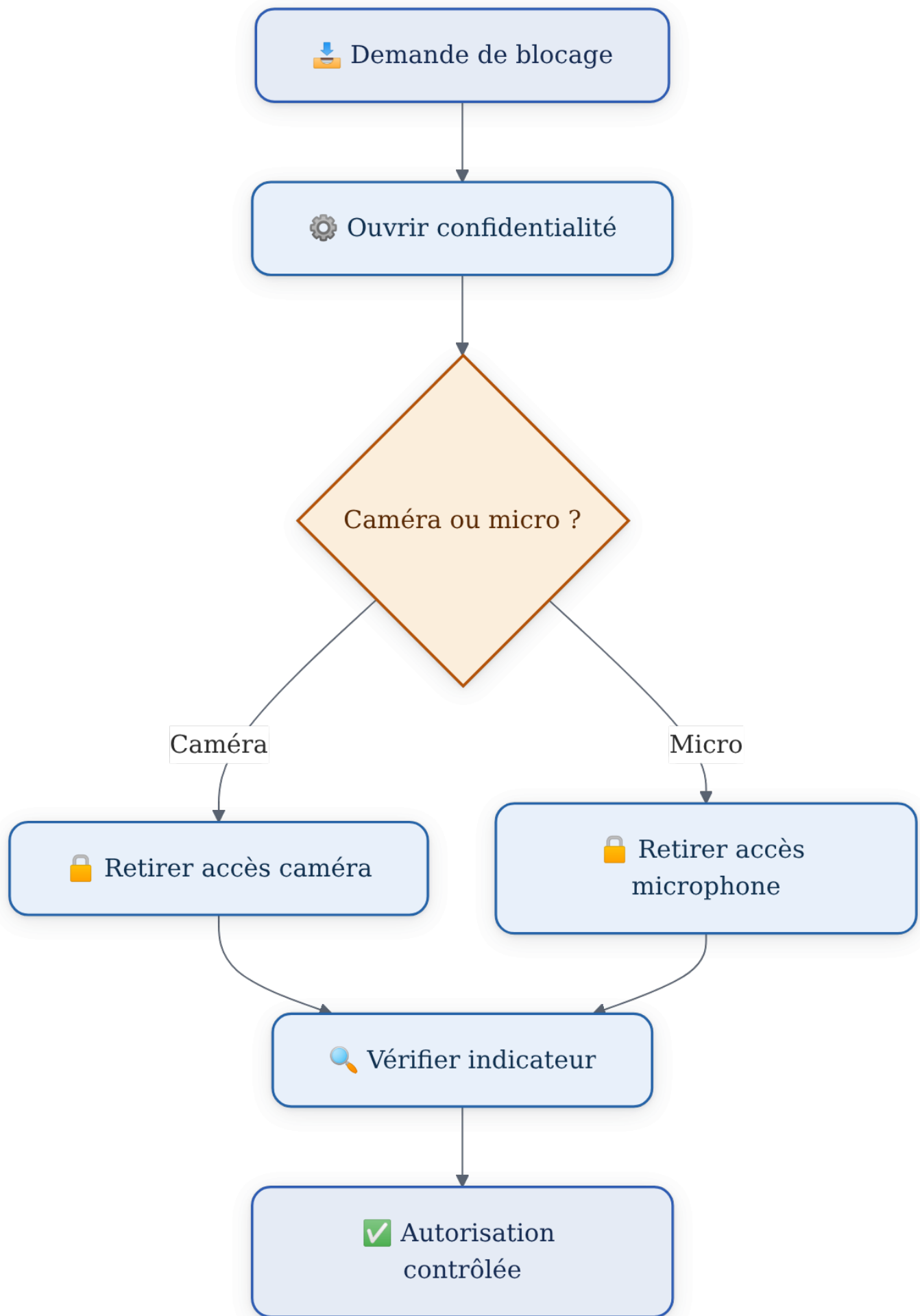
- 1 1. Identifier un accès à vérifier
- 2 2. Retirer les autorisations sur téléphone ou tablette
- 3 3. Bloquer les accès sur ordinateur et dans le navigateur
- 4 4. Choisir l'autorisation adaptée à chaque situation
- 5 5. Tester et garder le contrôle

1. Identifier un accès à vérifier

- ☐ **Observer l'indicateur d'activité de la caméra ou du microphone.**
Un indicateur inattendu doit déclencher une vérification.
- ☐ **Noter l'application ouverte au moment où l'indicateur apparaît.**
- ☐ **Fermer les applications de visioconférence, d'enregistrement audio et de navigation vocale non utilisées.**
- ☐ **Vérifier si la fonction de l'application justifie réellement l'accès à la caméra ou au micro.**

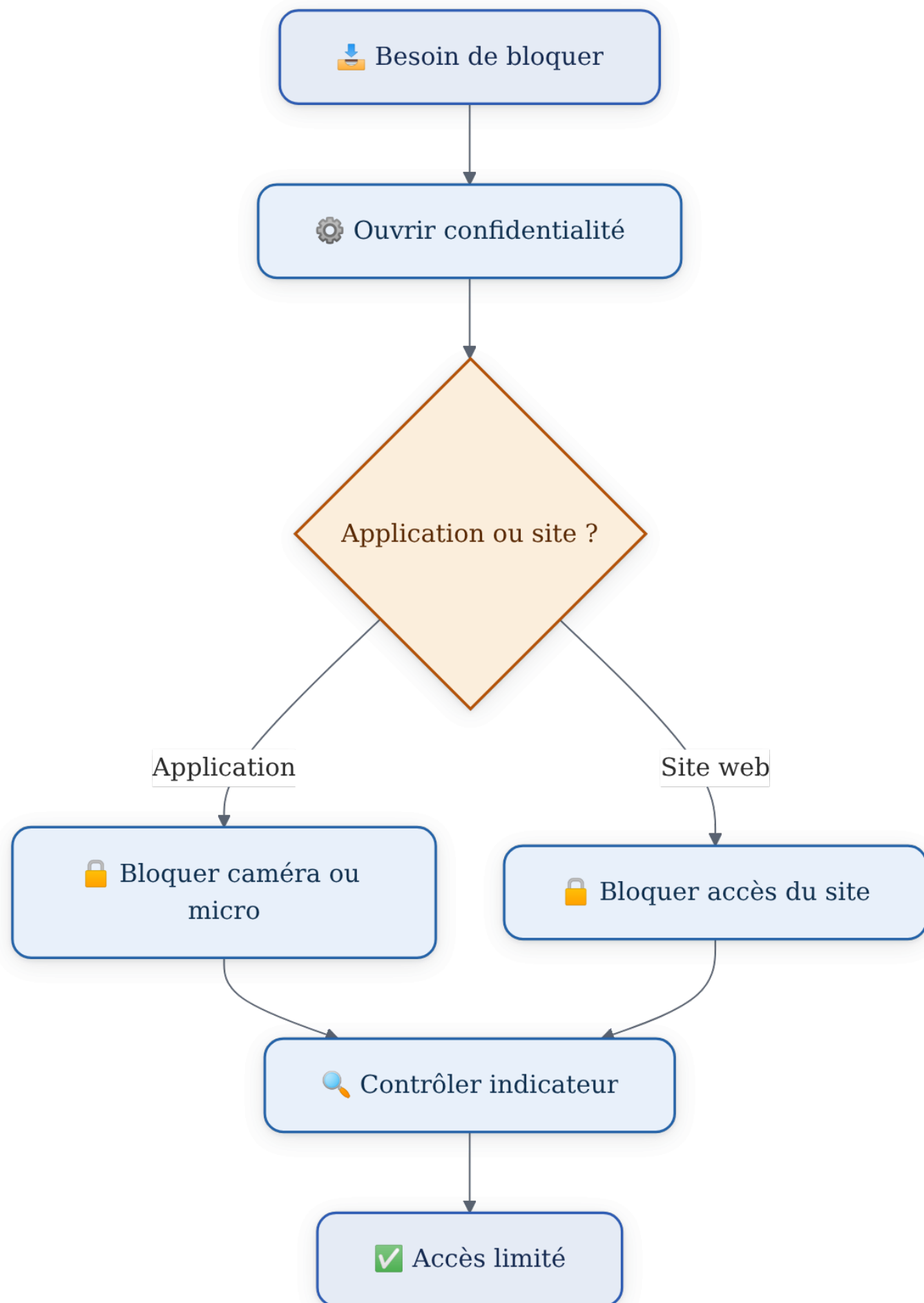
2. Retirer les autorisations sur téléphone ou tablette

- ☐ **Ouvrir les réglages de confidentialité ou la fiche de l'application ciblée.**
- ☐ **Consulter séparément les rubriques Caméra / Appareil photo et Microphone.**
- ☐ **Désactiver l'accès à la caméra si l'application n'a pas besoin de prendre des images.**
- ☐ **Désactiver l'accès au microphone si l'application n'a pas besoin d'enregistrer ou de transmettre du son.**
- ☐ **Choisir une autorisation limitée dans le temps lorsqu'elle est proposée et nécessaire.**
Par exemple, uniquement pendant l'utilisation ou à chaque demande.
- ☐ **Éviter de modifier les autorisations des autres applications sans raison.**



3. Bloquer les accès sur ordinateur et dans le navigateur

- ☐ Ouvrir les paramètres de confidentialité du système.
- ☐ Examiner séparément les autorisations Caméra et Microphone.
- ☐ Retirer l'accès de l'application concernée plutôt que bloquer sans distinction les outils nécessaires.
- ☐ Vérifier les autorisations accordées aux applications de bureau et aux services système lorsqu'ils sont listés.
- ☐ Contrôler aussi les permissions du site web dans le navigateur.
L'autorisation d'un site est distincte de celle de l'application ou du système.
- ☐ Retirer l'autorisation d'un site qui n'a pas besoin de caméra ou de microphone.



4. Choisir l'autorisation adaptée à chaque situation

Situation	Réflexe recommandé
Visioconférence en cours	Autoriser caméra et micro seulement si nécessaires à l'appel, puis révéifier après usage.
Application sans besoin évident de capteurs	Refuser l'accès à la caméra et au microphone.
Besoin ponctuel de prendre une photo ou d'enregistrer du son	Accorder l'accès le plus limité proposé par le système.
Site web ouvert dans un navigateur	Vérifier son autorisation propre, même si l'application navigateur est autorisée.
Indicateur actif sans explication	Identifier l'application active, fermer ce qui est inutile et examiner les permissions.

5. Tester et garder le contrôle

- ☐ Fermer puis rouvrir l'application après avoir modifié une permission.
- ☐ Lancer la fonction qui utilisait auparavant la caméra ou le micro.
- ☐ Vérifier que l'accès est refusé, qu'une demande apparaît ou que la capture ne démarre pas.
- ☐ Réactiver uniquement l'autorisation indispensable si l'application ne peut pas fonctionner sans elle.
- ☐ Revoir régulièrement les applications installées et leurs permissions.

! À retenir

Bloquer une permission limite ce qu'une application peut utiliser, mais ne garantit pas à lui seul l'absence de logiciel malveillant. Privilégiez les réglages natifs du système et restez attentif aux accès qui ne correspondent pas à l'usage de l'application.

Les intitulés et emplacements des réglages peuvent varier selon l'appareil, le fabricant, la version du système et le navigateur.